11

Method and apparatus for controlling the dissemination of digital information.

Patent Number:	EP0672991, A3, B1
Publication date:	1995-09-20
Inventor(s):	KANKANHALLI MOHAN S (SG); NARASIMHALU ARCOT D (SG); WANG WEIGUO (SG)
Applicant(s)::	INST OF SYSTEMS SCIENCE (SG)
Requested Patent:	DE69502526T
Application Number:	EP19950301630 19950313
Priority Number(s):	US19940210174 19940317
IPC Classification:	G06F17/60 ; G07F17/00 ; H04L9/32
EC Classification:	G07F17/16, H04N7/167D
Equivalents:	DE69502526D, US5499298

Abstract

The present invention is a method and apparatus for controlling the dissemination of digital information. Digital information is structured logically to incorporate usage history and allowable access window before it is encrypted in a header portion and a body portion. The end user accesses the digital information with a tamper-proof controlled information access device by decrypting the digital information. A controller disposed in the controlled information access device permits end users to access transparently uncontrolled information. Controlled digital information will be accessed as long as the conditions specified by the information provider are met. In one embodiment of the present invention, controlled information is disseminated in an off-line manner while the second embodiment of the present invention disseminates controlled digital information in an on-line manner.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Übersetzung der europäischen Patentschrift

(87) EP 0 672 991 B1

(10) DE 695 02 526 T 2

(51) Int. Cl.[6]:
G 06 F 17/60
G 07 F 17/00
H 04 L 9/32
G 06 F 1/00

(21) Deutsches Aktenzeichen: 695 02 526.0
(86) Europäisches Aktenzeichen: 95 301 630.0
(86) Europäischer Anmeldetag: 13. 3. 95
(87) Erstveröffentlichung durch das EPA: 20. 9. 95
(87) Veröffentlichungstag der Patenterteilung beim EPA: 20. 5. 98
(47) Veröffentlichungstag im Patentblatt: 21. 1. 99

(30) Unionspriorität:
210174 17. 03. 94 US

(73) Patentinhaber:
Institute of Systems Science, Kent Ridge, SG

(74) Vertreter:
G. Koch und Kollegen, 80339 München

(84) Benannte Vertragstaaten:
DE, GB

(72) Erfinder:
Narasimhalu, Arcot D., Singapore 1129, SG; Wang, Weiguo, Singapore 1027, SG; Kankanhalli Mohan S., Kankanhalli Mohan S., Singapore 1027, SG

(54) Verfahren und Vorrichtung zur Kontrolle der Verbreitung von digitaler Information

- kein Watermarking
- keine Personalisierung
- Überwiegend Kontrolle der Zahl von Zugriffen und Gültigkeitsdauer einer Berechtigung

DE 695 02 526 T 2

DE 695 02 526 T 2

95301630.0
EP 0672991

Beschreibung:

Hintergrund der Erfindung

1. Gebiet der Erfindung

Die vorliegende Erfindung bezieht sich auf das Gebiet der Datenverarbeitung und insbesondere auf ein Verfahren und eine Vorrichtung zur Steuerung der Verbreitung von digitaler Information. Weiterhin ergibt die vorliegende Erfindung einen transparenten Zugriff auf nicht-kontrollierte digitale Information zusammen mit kontrollierter digitaler Information mit der gleichen Zugriffsvorrichtung.

2. Beschreibung des verwandten Standes der Technik

Die Verteilung von Originalwerken - unabhängig davon, ob diese Text, Grafik, Animation, Video oder Audio darstellen - auf magnetischen, elektronischen, optischen oder irgendwelchen anderen Medien wird zunehmend popolär. Fortschritte in der digitalen Kompressionstechnologie und Verbesserungen des Preis-Leistungsverhältnisses von Computern haben es wirtschaftlich und sinnvoll gemacht, digitale informationen in derartigen "Soft"-Formen zu verbreiten. In einem digitalen Medium codierte Originalwerke können jedoch sehr einfach kopiert, verschlüsselt, über Kommunikationsnetze übertragen und gelöscht werden. Für die folgende Beschreibung der vorliegenden Erfindung werden in einem digitalen Medium codierte Originalwerke als digitale Informationen bezeichnet. Die Vorteilsfaktoren, d.h. leichter Zugang und Manipulation, die digitale Information zu einem Rivalen für traditionelle Hardcopy-Formate gemacht haben, d.h. Bücher, Zeitungen und Microfiches, haben es auch schwierig gemacht, einen Nachweis einer illegalen Benutzung einer derartigen Information festzustellen.

Hinsichtlich der Verteilung von Papierkopien von Originalwerken bilden Urheberrecht und Veröffentlichungsgesetz einen Ausgleich zwischen den gleichzeitigen Zielen der Vergütung des Herausgebers/Autors und der Aufrechterhaltung annehmbarer Kosten für die Endbenutzer. Es ist sehr einfach, einen Nachweis der Herstellung illegaler Kopien von Papierkopien von Originalwerken zu führen. Die Hauptstoßrichtung von Urheberrechts- und Veröffentlichungsgesetzen besteht in dem Führen eines Nachweises des illegalen Besitzes.

Im Gegensatz hierzu ist der Nachweis eines illegalen Besitzes von digitaler Information zumindest schwierig und im Schlimmstfall unmöglich zu führen. Die vorliegende Erfindung schlägt vor, die Benutzung von verteilter digitaler Information als eine Alternative zu kontrollieren. Mit dem Wort Benutzung wird in der vorliegenden Erfindung die Anzahl und die Zeit der Zugriffe, die von dem Informationslieferanten festgelegt sind, bezeichnet.

Der Stand der Technik kontrolliert nur die Verbreitung von Softwareprogrammen mit Kopierschutzschemas. Der Kopierschutz beruht auf Hardeware- oder Software-Artifakten, um das illegale Kopieren von Softwareprogrammen festzustellen und zu verhindern. Eine Verschlüsselung wird in manchen Fällen verwendet, um einen Kopierschutz zu schaffen. Einige neuere Beispiele von Kopierschutzschemen sind in dem US-Patent 4 866 769 auf den Namen von Karp und dem US-Patent 4 903 296 auf den Namen Chandra et al. angegeben.

Das US-Patent 4 903 296 beansprucht den Kopierschutz von Software auf einem magnetischen Medium mit einem speziellen Schlüssel, der zwei Markierungen aufweist, die auf der Oberfläche des Mediums hergestellt ist. Diese Markierungen weisen die Form eines Fehlens von Material und Domänen auf, die von üblichen magnetischen Plattenschreibköpfen nicht gebildet werden können. Zusätzlich wird ein Verschlüsselungs-Schlüssel, der kritisch für den Betrieb der Anwendung ist, in ein Spezialzweck-Hardware-Teilsystem eingebaut. Schließlich ist das Hardware-Teilsystem zum Entschlüsseln des Schlüssels erforderlich.

Das US-Patent 4 866 769 lehrt ein Verfahren zum Kopierschutz von Personalcomputer-Software, die auf Disketten verteilt wird, mit Hilfe der Verwendung einer eindeutigen Information, die im Festwertspeicher eines Personalcomputers gespeichert ist. Eine Quellen-ID (Identifikation) wird mit jeder verteilten Software geliefert. Die Identifikation ID des Personalcomputers wird zusammen mit der Quellen-ID auf der Verteilungsdiskette verwendet, um ein codiertes Prüfwort zu erzeugen, wobei irgendein verfügbares Verschlüsselungsverfahren verwendet wird. Dieses Prüfwort wird dann dazu verwendet, zu überprüfen, daß die Software auf dem hierfür bestimmten Personalcomputer verwendet wird.

Während die US-Patente 4 903 296 und 4 866 769 Offline-Schemas für die kontrollierte Verbreitung von Software beschreiben, beschreibt das US-Patent 4 999 806 eine Zentralstation, die Software über Telefonleitungen verteilt - ein Online-Schema für die Software-Verbreitung. Die Zentralstation überträgt einen Annahmecode an einen Anrufer und beendet dann den Anruf. Nach der Überprüfung der Kreditinformation des Anrufers ruft die Zentralstation den Käufer zurück und setzt die Transaktion lediglich nach dem Empfang des Annahmecodes fort. Die Zentralstation überträgt dann ein Steuerungsübergabeprogramm und ein Initialisierungsprogramm an den Käufer. Der Käufer führt das Initialisierungsprogramm aus, um die Steuerung des Computers des Käufers auf die Zentralstation zu übergeben. Das Steuerungsübergabeprogramm stellt sicher, daß keine speicherresidenten Kopierprogramme laufen, bevor es über die Telefonleitung das gekaufte/gemietete Programm auf den Rechner des Käufers überträgt. Danach werden die verschiedenen übertragenen Programme gelöscht, wobei lediglich eine Kopie der geschützten Version des gekauften Programms auf der Festplatte des Käufers zurückbleibt.

Um das nichtautorisierte Kopieren und den nichtautorisierten Gebrauch von Informationen zu verhindern, erfordern bekannte Kopierschutzschemas entweder die Einführung künstlicher Indizes als Softwareschlüssel oder spezielle Hardware-Teilsysteme. Diese Lösungen sind nicht nur sowohl für die Informations-

lieferanten als auch die Endbenutzer kostspielig, weil sie zusätzliche Verarbeitungsschritte erfordern, sondern sie sind auch nicht mit dem Trend der Förderung der gleichzeitigen Verwendung von unterschiedlichen Informationsarten in einer Netzwerkumgebung vereinbar. Weiterhin ergeben die bekannten Kopierschutzschemas eine beschränkte Kontrolle über die Verbreitung von digitaler Information, weil sie zwar das nicht-autorisierte Kopieren von Software, nicht jedoch den nicht-autorisierten "Gebrauch" derartiger Information verhindern.

In dem Stand der Technik fehlt die Verbreitung von nicht-kontrollierter Information. Der Begriff "nicht-kontrollierte Information" bezieht sich bei der vorliegenden Erfindung auf einen Teil der Information, für die der Informationslieferant beschlossen hat, daß sie der Endverbraucher betrachten kann, ohne daß er dies als einen "Gebrauch" der kontrollierten Information registriert. Typischerweise weist die nicht kontrollierte Information entweder eine niedrigere Auflösung verglichen mit der kontrollierten Information auf, oder sie umfaßt einen ausgewählen Teil der kontrollierten Information, der es dem Endverbraucher ermöglicht, eine informierte Entscheidung zu machen, ob er an dieser kontrollierten Information teilhaben oder diese verwenden will. Beispiele von nicht kontrollierter Information sind die Vorschau auf einen Kinofilm oder eine Vorführversion der kontrollierten Software oder sogar die Zusammenfassung eines Patentdokumentes. Bisherige bekannte Informationsverbreitungssysteme ermöglichen nicht den transparenten Zugriff auf nicht-kontrollierte digitale Information mit der gleichen Zugriffseinrichtung wie der, die für den Zugriff auf die kontrollierte digitale Information verwendet wird.

In den Veröffentlichungen "The Concept of a Software Service System (SSS)" und "Implementation of a Small-Scale Prototype for Software Service System (SSS)" von Mori und Tashiro, Systems and Computers in Japan, Band 19, Nr. 5, 1988, Seiten 38-60 ist ein Software-Lizensierungssystem beschrieben, bei dem Software-Zugriffsrechte in einem Anfangsblock verschlüsselt

werden, der mit der Software verteilt wird. Bei diesem SSS-System wird jede Modifikation von Zugriffsrechten (beispielsweise Herunterschalten eines die Anzahl der Zugriffe zählenden Zählers) unter Verwendung einer speziellen betrugssicheren "SSS-Box" durchgeführt.

Zusammenfassung der Erfindung

Die vorliegende Erfindung bezieht sich auf ein Verfahren zur Kontrolle der Verbreitung von digitaler Information, wie es im Anspruch 1 und Anspruch 4 angegeben ist.

Kurze Beschreibung der Zeichnungen

Figur 1 ist ein Modell der Informationsverbreitung,

Figur 2 zeigt eine logische Struktur einer Gesiegelten Kontrollierten Information (COIN) gemäß einer ersten Ausführungsform der vorliegenden Erfindung,

Figur 3 zeigt die Architektur eines Gerätes, das von einem Informationsverbraucher zum Zugriff auf die kontrollierte Information verwendet wird, gemäß der ersten Ausführungsform der vorliegenden Erfindung,

Figur 4 zeigt das logische Ablaufdiagramm, wie die Gesiegelte COIN von einem Informationslieferanten zubereitet wird,

Figuren 5A und 5B zeigen den logischen Ablauf des Steuergerätes in der Zugriffsvorrichtung gemäß der ersten Ausführungsform der vorliegenden Erfindung,

Figur 6 zeigt die Architeektur eines Zugriffsgerätes für ein System zur kontrollierten Verbreitung von digitaler Information gemäß der zweiten Ausführungsform der vorliegenden Erfindung,

Figur 7A zeigt ein mögliches Format der logischen Struktur von Gesiegelter COIN, wie es bei einer zweiten Ausführungsform der vorliegenden Erfindung verwendet wird,

Figur 7B zeigt ein mögliches Format der logischen Struktur des Gesiegelten Öffners, der mit der Gesiegelten COIN zusammenwirkt, die bei der zweiten Ausführungsform der vorliegenden Erfindung verwendet wird,

Figur 8 zeigt das Ablaufdiagramm des Informationslieferanten, das bei der zweiten Ausführungsform der vorliegenden Erfindung verwendet wird, bei dem eine Gesiegelte COIN erzeugt wird,

Figur 9 zeigt das Ablaufdiagramm des Informationslieferanten, das bei der zweiten Ausführungsform der vorliegenden Erfindung verwendet wird, bei der ein Öffner für den Zugriff auf die gesiegelte COIN in Figur 8 erzeugt wird,

Figur 10 zeigt den logischen Ablauf des Gesamtverfahrens einer Online-gesteuerten Verbreitung von Information gemäß der zweiten Ausführungsform der vorliegenden Erfindung,

Figuren 11A und 11B zeigen das Ablaufdiagramm des Steuergerätes bei dem Zugriffgerät gemäß der zweiten Ausführungsform der vorliegenden Erfindung.

Ausführliche Beschreibung der Erfindung

Ein Verfahren und eine Vorrichtung zur Steuerung der Verbreitung von digitaler Information wird beschrieben. In der folgenden Beschreibung werden verschiedene spezielle Einzelheiten dargelegt, wie z.B. logische Strukturen der digitalen Information und Programmschritte usw., um ein vollständiges Verständnis der vorliegenden Erfindung zu schaffen. Es ist für den Fachmann offensichtlich, daß die vorliegende Erfindung ohne diese speziellen Einzelheiten durchgeführt werden kann. In anderen Fällen werden gut bekannte Schritte, wie sie z.B. bei

der Verschlüsselung und Entschlüsselung von Daten verwendet werden, nicht gezeigt, um die vorliegende Erfindung nicht unklar zu machen.

Schreibweise und Bezeichnungen

Eine ausführliche Beschreibung bezüglich der kontrollierten Verbreitung von digitaler Information wird teilweise in Ausdrücken von Algorithmen und einer symbolischen Darstellung von Operationen an Datenbits in einem Computerspeicher dargeboten. Diese algorithmischen Beschreibungen und Darstellungen sind die Mittel, die von dem Fachmann auf dem Gebiet der Datenverarbeitung verwendet werden, um den Inhalt ihrer Arbeit anderen Fachleuten in wirkungsvoller Weise zu übermitteln.

Ein Algorithmus wird hier und allgemein als eine in sich abgeschlossene Folge von Schritten aufgefaßt, die zu einem gewünschten Ergebnis führen. Diese Schritte erfordern die physikalische Manipulation von physikalischen Größen. Üblicherweise, jedoch nicht notwendigerweise, nehmen diese Größen die Form von elektrischen, optischen oder magnetischen Signalen an, die gespeichert, übertragen, kombiniert oder auf andere Weise manipuliert werden können. Es erweist sich zu gewissen Zeiten als bequem, hauptsächlich aus Gründen des allgemeinen Gebrauchs, auf diese Signale als Bits, Werte, Elemente, Symbole, Zeichen, Ziffern oder dergleichen Bezug zu nehmen. Es sei jedoch hierbei berücksichtigt, daß alle diese und ähnliche Ausdrücke mit den passenden physikalischen Größen in Verbindung gebracht werden sollen und diese Begriffe lediglich bequeme Bezeichnungen sind, die auf diese Größen angewandt werden.

Weiterhin werden die durchgeführten Manipulationen in vielen Fällen mit Ausdrücken bezeichnet, wie z.B. addieren oder vergleichen, die üblicherweise den mentalen Operationen zugeordnet werden, die von einem Menschen durchgeführt werden. Keine derartige Fähigkeit eines Menschen ist erforderlich oder wünschenswert. In den meisten Fällen sind bei allen hier beschriebenen Operationen, die einen Teil der vorliegenden Erfindung bilden,

die Operationen Maschinenoperationen. Brauchbare Maschinen zur Durchführung der Operationen der vorliegenden Erfindung schließen Allzweck-Digitalrechner oder ähnliche Geräte ein. In allen Fällen sollte berücksichtigt werden, daß ein Unterschied zwischen der Verfahrensoperation beim Betrieb eines Rechners oder anderen Vorrichtungen und dem Berechnungsverfahren selbst besteht. Die vorliegende Erfindung bezieht sich auf Verfahrensschritte zur Schaffung einer besseren Kontrolle über die Verbreitung digitaler Information.

Die vorliegende Erfindung bezieht sich weiterhin auf eine Vorrichtung zur Durchführung dieser Operationen. Diese Vorrichtung kann speziell für den erforderlichen Zweck konstruiert sein, oder sie kann einen Allzweck-Rechner umfassen, der selektiv durch ein Computerprogramm aktiviert oder umkonfiguriert wird, das in dem Rechner gespeichert ist. Die hier gelieferten Algorithmen sind nicht von Natur aus auf irgendeinen speziellen Computer oder eine andere Vorrichtung bezogen. Insbesondere können verschiedene Allzweckmaschinen mit Programmen verwendet werden, die gemäß den hier gegebenen Lehren geschrieben sind, oder es kann sich alls zweckmäßiger erweisen, spezielle Vorrichtungen zu konstruieren, wie z.B. einen Spezialzweck-Prozessor, um die erforderlichen Verfahrensschritte auszuführen. Die erforderliche Struktur für eine Vielzahl dieser Maschinen sollte aus der nachfolgenden Beschreibung ersichtlich sein.

ALLGEMEINE SYSTEMKONFIGURATION

Ein allgemeines Modell der Informationsverbreitung ist in Figur 1 gezeigt. Hier bezeichnet der Informationslieferant 10 einen Lieferanten von allen Arten von Information unter Einschluß von, jedoch ohne Beschränkung auf, Information in Form von Text, Graphik, Animation, Video, Audio, Software oder irgendeiner Kombination hiervon. Der Übertragungskanal 20 stellt die Einrichtung und insbesondere das Medium dar, über das Information dem Informationsverbraucher 30 über Pfade 15 und 25 geliefert wird. Der Übertragungskanal 20 schließt ohne jede Beschränkung irgendeine Kommunikationseinrichtung oder ein

Kommunikationsmedium, wie Computernetze, Satellitenstrecken, Disketten, optische Platten oder andere Speichermedien ein. Es sei weiterhin für den Fachmann verständlich, daß der Informationsverbraucher 30 austauschbar mit einem oder mehreren Endbenutzern von Informationen verwendet wird. Die vorliegende Erfindung wählt das Wort "Informationsverbraucher", um die einmalige Art der Verwendung der kontrollierten Information hervorzuheben. Dies heißt mit anderen Worten, daß sobald die kontrollierte Information einmal verbraucht ist, die ursprüngliche Information nicht mehr in brauchbarer Form vorliegt und der erneute Zugriff auf die gleiche Information nicht automatisch ist. Die einmalige Art des Gebrauchs kann als n-facher Gebrauch verallgemeinert werden, d.h., sobald die kontrollierte Information n mal verwendet wurde, existiert sie nicht mehr länger in brauchbarer Form.

Die Erfindung lehrt Verfahren und Vorrichtungen für einen Informationslieferanten zur Erstellung einer Informationspackung zur Verbreitung. Diese Verfahren werden im folgenden mit speziellen Schritten der Manipulation von Informationen beschrieben. Für den Fachmann ist es offensichtlich, daß einige dieser Schritte am besten zu automatisieren sind, beispielsweise indem sie in Form einer Spezialzweck-Software implementiert werden, der normalerweise als ein Server bezeichnet wird und auf Allzweckrechnern läuft. Es ist weiterhin klar, daß ein Informationslieferant gleichzeitig mehrfache Ausführungen des Servers einleiten könnte, um mehrere Informationsverbraucher zu bedienen. Aus Gründen der Klarheit der Darstellung erfolgt die Beschreibung an dem Modell, das einen Lieferanten und einen Verbraucher hat. Es ist weiterhin klar, daß ein Informationsverbraucher außerdem ein weiterer Informationslieferant sein kann.

ERSTE AUSFÜHRUNGSFORM DER VORLIEGENDEN ERFINDUNG

1. Erstellung des Verteilungspaketes

Figur 2 zeigt eine logische Struktur einer Gesiegelten Kon-

trollierten Information (COIN) gemäß einer ersten Ausführungsform der vorliegenden Erfindung. Die Gesiegelte COIN wird von einem Informationslieferanten erstellt, sobald der Informationsverbraucher den Bedingungen eines Informationsverteilungsvertrages zustimmt. Die erste Ausführungsform der vorliegenden Erfindung beschreibt ein Offline-Schema, bei dem der Übertragungskanal 20 irgendeine Art von nichtflüchtigem Speichermedium umfaßt, beispielsweise eine Diskette, eine Festplatte, eine optische Platte und andere nicht-flüchtige Halbleiter-Speicherbauteile. Ein Informationsverteilungsvertrag enthält zumindest die Identität der kontrollierten Information, die Anzahl der Zugriffe und die Art des Übertragungsmediums 20.

Gemäß Figur 2 umfaßt die logische Struktur der Gesiegelten Kontrollierten Information (COIN) einen Anfangsblock 35 und einen Hauptteil 40. COIN bezieht sich auf die ursprüngliche Information, die in irgendeiner "weichen" Form codiert ist (beispielsweise elektronisch, magnetisch oder optisch) und die der Informationslieferant 10 dem Informationsverbraucher 30 für dessen Zugriff für eine vorgegebene Anzahl von Fällen liefert. COIN wird unter Verwendung irgendeines Schemas derart codiert oder gesiegelt, daß ein Zugriff auf die COIN ohne einen gültigen Entschlüsselungs-Schlüssel vom Rechenaufwand her unmöglich ist. Der Anfangsblock 35 umfaßt eine Vielzahl von Feldern: eine Medium-Signatur 36, ein Zugriffsfenster 37 (AW), die Gesamtzahl der zugelassenen legalen Zugriffe 38 (TAL), die Anzahl der verbleibenden legalen Zugriffe 39 (LAL) und TAL, die Anzahl der Verschlüsselungs-/Entschlüsselungsschlüssel 41 (K_1 bis K_{TAL}). Die Medium-Signatur 36 bezieht sich auf irgendein Schema, das es einem Verteilungsmedium, wie z.B. einer Diskette, ermöglicht, eine eindeutige Identifikation zu haben. Vorzugsweise hängt diese Signatur von den Eigenschaften oder Ungleichförmigkeiten des Verteilungsmediums ab. Bezüglich eines Beispiels für eine geeignete Medium-Signatur sei auf die anhängige US-Patentanmeldung 08/120 969 vom 13. September 1993 auf den Namen des gleichen Anmelders wie die vorliegende Anmeldung verwiesen. Die AW 37 bezieht sich

auf eine festgelegte Zeitperiode, innerhalb der dem Informationsverbraucher ein legaler Zugriff für den Zugriff auf die COIN gewährt wird. Es ist eine Anfangs- und Endzeit als Begrenzung des Zugriffsfensters angegeben, innerhalb dessen der Informationsverbraucher 30 in legaler Weise einen Zugriff auf die verbreitete Information ausführen kann. TAL 38 ist die Gesamtzahl von legalen Zugriffen auf die COIN, die der Informationslieferant 10 dem Informationsverbraucher 30 unter einem Informationsverbreitungsvertrag gewährt. LAL 39 ist die Anzahl der verbleibenden legalen Zugriffe, sie ist die Differenz zwischen TAL und der Anzahl von bereits gewährten Zugriffen. Wenn LAL gleich Null ist, wird ein Zugriff auf die COIN verweigert. K_1 bis $K_{TAL}41$ sind Schlüssel, die zum Entschlüsseln der COIN in dem Hauptteil 40 verwendet werden. Das Verschlüsselungs- und Entschlüsselungsschema von K_1 bis $K_{TAL}41$ beruht auf der Verschlüsselung mit öffentlichem Schlüssel (PKC), die es dem Informationslieferanten ermöglicht, geheime Nachrichten an das Zugriffsgerät ohne vorherige Übertragung eines geheimen Schlüssels zu übertragen. Unter PKC hat jede Partei zwei Schlüssel - einen geheimen (der der Partei lediglich selbst bekannt ist) und einen öffentlichen Schlüssel (der jedem bekannt ist, ähnlich wie eine Telefonnummer in einem Telefonverzeichnis). Dies heißt mit anderen Worten, daß der Informationslieferant einen geheimen Schlüssel (SSK) und einen öffentlichen Schlüssel (SPK) hat, während das Zugriffsgerät einen geheimen Schlüssel (DSK) und einen öffentlichen Schlüssel (DPK) hat. Wenn der Informationslieferant eine geheime Nachricht an den Informationsverbraucher sendet, verwendet der Informationslieferant den öffentlichen Schlüssel (DPK) des Zugriffsgerätes zur Verschlüsselung der Nachricht. Lediglich das Zugriffsgerät kann die verschlüsselte Nachricht unter Verwendung seines eigenen geheimen Schlüssels (DSK) entschlüsseln. Zur weiteren Bezugnahme auf PKC wird auf R.L. Rivest, A. Shamir und L. Adleman: "A Method for Obtaining Digital Signature in Public-Key Cryptosystems", Communications of the ACM, Band 21, Nr. 2, Februar 1978, Seiten 120 - 126 verwiesen. Siehe auch D.E.R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, MA, 1983.

Sobald sich der Informationsverbraucher 30 mit dem Informationslieferanten 10 hinsichtlich der Bedingungen des Verteilungsvertrages geeinigt hat, führt de Informationslieferant 10 ein Verfahren aus, wie es in Figur 4 umrissen ist, und zwar beginnend mit dem Schritt 60 zur Erzeugung eines Verteilungsmediums, das die gesiegelte COIN beinhaltet. Im Schritt 62 wird die Anzahl TAL von Schlüsseln K_1 bis K_{TAL} erzeugt, um die COIN in dem Hauptteil 40 zu verschlüsseln. Obwohl bei der Ausführungsform der vorliegenden Erfindung auf PKC Bezug genommen wird, ist jedes Verschlüsselungsverfahren anwendbar. Als nächstes wird eine Medium-Signatur 36 aus dem speziellen Verteilungsmedium geschaffen, auf dem die COIN verteilt werden soll. Die anhängige US-Anmeldung 08/120 969 vom 13. September 1993, die auf den gleichen Anmelder wie die vorliegende Erfindung übertragen ist, gibt eine von vielen Möglichkeiten zur Erzeugung einer Medium-Signatur an. Im Schritt 66 wird COIN mit K_1 verschlüsselt. Hierauf wird der Hauptteil 40 der Gesiegelten COIN erzeugt. Im Schritt 68 wird der Anfangsblock 35 als nächstes erstellt. Zu Anfang wird der Wert LAL 39 so eingestellt, daß er identisch mit dem von TAL 38 ist. Durch Verknüpfen von AW 37, TAL 38, LAL 39, K_1 bis K_{TAL}41 und der Medium-Signatur 36 nach Figur 2 wird der Anfangsblock 35 dann im Schritt 68 verschlüsselt, wobei der öffentliche Schlüssel DPK des Zugriffsgerätes des Informationsverbrauchers verwendet wird. Der verschlüsselte Anfangsblock 35 und der verschlüsselte Hauptteil 40 bilden die Gesiegelte COIN und werden auf das Verteilungsmedium im Schritt 70 geschrieben.

2. Zugriff auf die Information

Es wird angenommen, daß der Informationsverbraucher 30 irgendein Gerät, beispielsweise einen Computer hat, um einen Zugriff auf die Information in dem verteilten Medium durchzuführen. Die minimalen Zusätze für ein derartiges Gerät für den Zugriff auf COIN sind in Figur 3 gezeigt. Das Steuergerät 45 ist an seinem Eingang mit einem Informationseingangskanal 27 zum Empfang verbreiteter Informationen von dem (nicht gezeigten) Lesegerät

des verteilten Mediums gekoppelt. Das Steuergerät ist weiterhin an einem seiner Ausgänge mit einem Informationsausgangskanal 29 zur Übertragung von neu verschlüsselter Information an das (nicht gezeigte) Schreibgerät des verteilten Mediums gekoppelt. Die Funktion des Steuergerätes 45 wird weiter unten bei der Beschreibung der Figur 5 beschrieben. Es sollte für den Fachmann verständlich sein, daß das Steuergerät 45 vollständig in Form von Hardware oder durch einen Allzweckprozessor mit geeigneter Software gerätemäßig ausgeführt werden kann. Das Steuergerät ist weiterhin an dem anderen Ausgang mit einer Ausgangseinheit 50 über eine Verbindungsstrecke 47 zur Anzeige der verbreiteten Information gekoppelt. Die Ausgangseinheit 50 könnte eine Anzeigeeinheit für Text/Graphik/Animation/Video oder ein Wandler für Audioinformation sein. Die Ausgangseinheit 50 selbst könnte ein Gerät zur Verteilung kontrollierter Information an andere Informationsverbraucher sein. Das Steuergerät 45 ist weiterhin mit einer Uhr 55 über eine Verbindungsstrecke 49 gekoppelt, um eine Gegenprüfung durchzuführen, ob die Echtzeit innerhalb der Grenzen des Zugriffsfensters AW 37 liegt. Vorzugsweise sind die Uhr 55 und das Zugriffsgerät verfälschungssicher, so daß der Informationsverbraucher weder die Verbindungsstrecke 47 anzapfen noch den Wert der Uhr 55 ändern kann. Es sollte für den Fachmann verständlich sein, daß das Steuergerät Einrichtungen zur Wechselwirkung mit dem Benutzer aufweist, wobei die Einzelheiten diese Einrichtungen hier fortgelassen sind, um die Beschreibung der ersten Ausführungsform der vorliegenden Erfindung nicht zu beeinträchtigen.

Die Figuren 5A und 5B fassen den logischen Ablauf des Steuergerätes 45 des Zugriffsgerätes gemäß der ersten bevorzugten Ausführungsform der vorliegenden Erfindung zusammen. Wenn der Informationsverbraucher 30 einen Zugriff auf die gesiegelte COIN ausführen will, lädt er oder sie im Schritt 80 das Medium-Lese-/Schreib-Gerät mit dem (nicht gezeigten) Verteilungsmedium, das die gesiegelte COIN enthält. Das Steuergerät 45 des Zugriffsgerätes empfängt die von der Medium-Lese-/Schreib-Vorrichtung gelieferte Information über den Eingangskanal 45. Das Steuergerät 45 prüft im Schritt 82, ob die Information an

dem Eingangskanal 27 verschlüsselt ist. Wenn die Information nicht verschlüsselt ist, d.h. unkontrollierte Information ist, ermöglicht es das Steuergerät 45, daß die Information an dem Eingangskanal 27 direkt im Schritt 84 über die Verbindungsstrecke 47 zur Ausgangseinheit 50 gelangt. Wenn die Information an dem Eingangskanal 27 jedoch verschlüsselt oder kontrolliert ist, entschlüsselt das Steuergerät 45 den Anfangsblock 35 der Gesiegelten COIN, indem im Schritt 88 der geheime Schlüssel DSK des Zugriffsgerätes verwendet wird. Wie dies oben erwähnt wurde, ist der geheime Schlüssel DSK dem Informationsverbraucher unbekannt. Als nächstes prüft das Steuergerät 45 im Schritt 90, ob irgendwelche legale Zugriffe übriggeblieben sind, indem der Wert von LAL 38 auf Null überprüft wird. Wenn keine legalen Zugriffe verbleiben, ist der Wert von LAL 38 = 0, und im Schritt 92 wird ein Ausweich-Verarbeitungsmodul aufgerufen, das entweder den Informationszugriff verweigert oder den Inhalt des Mediums löscht. Der genaue Vorgang hängt von der speziellen Ausführungsform der Erfindung ab. Wenn der Wert von LAL größer als Null ist, vergleicht das Steuergerät 45 im Schritt 94 den Wert des Zugriffsfensters AW 37 mit der Zeit der Uhr 55. Wenn die derzeitige Zeit außerhalb der Begrenzungen des AW 37 fällt, wird das Ausweich-Verarbeitungsmodul im Schritt 92 aufgerufen. Anderenfalls prüft das Steuergerät 45 im Schritt 96, ob die Medium-Signatur 36 der von dem Eingangskanal 27 gelesenen Signatur und der des Ausgangskanals 29 entspricht. Wenn die Medium-Signatur 36 nicht übereinstimmt, wird die gesiegelte COIN auf einem kopierten Medium gespeichert. Ein Ausweich-Verarbeitungsmodul wie im Schritt 92 wird aufgerufen. Anderenfalls bestätigt das Steuergerät 45, daß der Informationsverbraucher 30 ein Recht hat, auf die Gesiegelte COIN auf dem Verteilungsmedium zuzugreifen.

Es dürfte für den Fachmann verständlich sein, daß es das Steuergerät des Zugriffsgerätes der vorliegenden Erfindung dem Informationsverbraucher ermöglicht, in transparenter Weise einen Zugriff auf nicht-kontrollierte und kontrollierte Information in einer Offline-Betriebsweise unter Verwendung des gleichen Zugriffsgerätes zuzugreifen. Obwohl die vorliegende Erfindung

die Aufgabe des Hin- und Herschaltens zwischen zumindest zwei Zugriffsgeräten vermeidet, ermöglicht sie es dem Informationslieferanten, nicht-kontrollierte und kontrollierte Information in einem Paket zu verteilen. Wenn dem Informationsverbraucher mehr Informationen zur Verfügung stehen, wird die Verwendung kontrollierter Information unter den Bedingungen des Informationslieferanten gefördert.

Nachdem das Steuergerät 45 feststellt, daß der Informationsverbraucher 30 ein Recht für einen Zugriff auf die gesiegelte COIN auf dem Verteilungsmedium hat, leitet gemäß Figur 5A das Steuergerät im Schritt 95 den Verschlüsselungs-/Entschlüsselungs-Schlüssel $K_{TAL - LAL + 1}$ von dem Anfangsblock 35 ab. Das Steuergerät 45 sperrt die Ausgabe der entschlüsselten Information über den Ausgangskanal 29. Das Steuergerät 45 entschlüsselt dann die gesiegelte COIN unter Verwendung des Schlüssels $K_{TAL - LAL + 1}$ im Schritt 98. Die entschlüsselte Information, COIN, wird im Schritt 100 gemäß Figur 5B als Ausgangssignal der Ausgangseinheit 50 über die Verbindungsstrecke 47 zugeführt. Hieraus folgt, daß der Informationsverbraucher 30 einen transparenten Zugriff auf die COIN ausführt, während das Steuergerät 45 automatisch die entsprechende kontrollierte Information prüft, gültig macht, verschlüsselt und entschlüsselt. Im Schritt 102 verkleinert das Steuergerät 45 den Wert von LAL um 1. Der Anfangsblock 35 wird somit zu einem modifizierten Anfangsblock 35'. Wenn der Wert von LAL gleich Null sein würde, wie dies im Schritt 104 geprüft wird, so wird ein "Sperre Informationszugriff"-Modul im Schritt 106 aufgerufen, das beispielsweise die Gesiegelte COIN auf dem Verteilungsmedium löscht. Wenn der Wert von LAL größer als Null ist, so extrahiert das Steuergerät 45 den Verschlüsselungs-/Entschlüsselungs-Schlüssel $K_{TAL - LAL + 2}$ und verschlüsselt die COIN im Schritt 108. Das Steuergerät 45 verschlüsselt dann den modifizierten Anfangsblock 35' unter Verwendung des öffentlichen Schlüssels DPK des Zugriffsgerätes. Schließlich schreibt das Steuergerät 45 die neue Gesiegelte COIN, die durch diese verschlüsselte COIN 40 und die Verschlüsselung des modifizierten Anfangsblockes 35' erzeugt

wurde, auf das Verteilungsmedium über den Ausgangskanal 29 im Schritt 110 zurück. Somit verwirklicht das in den Figuren 5A und 5B beschriebene Verfahren ein kontrolliertes Informationsschema für "n-fache Benutzung", das dem Informationslieferanten eine verbesserte Kontrolle über die Verbreitung digitaler Information gibt.

ZWEITE AUSFÜHRUNGSFORM DER VORLIEGENDEN ERFINDUNG

1. Gesamt-Systemaufbau und -Betriebsweise

Die zweite Ausführungsform der vorliegenden Erfindung beschreibt ein Online-Schema für die kontrollierte Verbreitung digitaler Information. Gemäß erneuter Bezugnahme auf die Figur 1 umfaßt der Übertragungskanal 20 eine Vielzahl von Kommunikationsstrecken zwischen dem Informationslieferanten 10 und dem Informationsverbraucher 30. Beispielsweise könnte der Übertragungskanal 20 ein Computernetz oder sogar Telefonleitungen einschließen.

Die Architektur eines Zugriffsgerätes, das ein Modell für den Informationsverbraucher 30 für ein Online-Schema bildet, ist in Figur 6 gezeigt. Kontrollierte Information von dem Übertragungkanal 20 wird dem Informationsverbraucher 30 über einen Eingangskanal 27 geliefert, der mit einem Steuergerät 48 gekoppelt ist. Die Funktionen des Steuergerätes 48 werden in Verbindung mit der Beschreibung von Figur 11 weiter erläutert. Das Steuergerät 48 kann entweder in Form von Hardware oder durch einen Allzweckprozessor mit geeigneter Sortware ausgeführt werden. Unter erneuter Bezugnahme auf Figur 6 ist zu erkennen, daß das Steuergerät 48 mit einer Ausgangseinheit 50 über einen freien Kanal 47 gekoppelt ist. Genauso wie bei der ersten Ausführungsform der vorliegenden Erfindung umfaßt die Ausgangseinheit 50 eine Vorrichtung zur Ausgabe kontrollierter Information oder einen Mechanismus zur Verteilung kontrollierter Information an andere. Das Steuergerät 48 ist weiterhin mit einer Speicherstufe 52 und einer Uhr 55 aus Gründen gekoppelt, die weiter unten erläutert werden. Das Steuergerät 48 ist mit

einem Ausgangskanal 29 zur Ausgabe von erneut verschlüsselter kontrollierter Information gekoppelt. Vorzugsweise sind die verschiedenen mit dem Steuergerät 48 gekoppelten Kanäle betrugssicher. Dies macht es unmöglich, daß Benutzer den freien Kanal 47 anzapfen, einen Zugriff auf das Steuergerät 48 ausführen, den Wert des Speichers 52 ändern oder den Wert der Uhr 55 ändern kann. Es ist für den Fachmann verständlich, daß das Steuergerät Einrichtungen zur Wechselwirkung mit dem Benutzer aufweist, wobei die Einzelheiten hiervon fortgelassen sind, um die Beschreibung der zweiten Ausführungsform der vorliegenden Erfindung nicht verwirrend zu machen.

Das Ziel des Online-Schemas der kontrollierten Verbreitung von digitaler Information besteht in der Erzielung einer verbesserten Kontrolle über die Zuführung von Information, so daß, sobald ein Zugriff auf die Information durch den Informationsverbraucher für eine festgelegte Anzahl von Malen ausgeführt wurde, die Information nicht mehr ohne Autorisierung von dem Informationslieferanten in einer brauchbaren Form existiert. Die verbesserte Kontrolle der Informationsverbreitung wird durch die Verwendung der Verschlüsselung und die Begrenzung des Zugriffs eines Informationsverbrauchers an einem bestimmten legalen Zugriffsgerät während eines Zugriffsfensters erzielt.

Um die obenerwähnten Kontrollen zu erzielen, ist die verschlüsselte COIN mit bestimmten Kontrolldaten gepackt, die als "Anfangsblock" bezeichnet werden, während die verschlüsselte COIN als der "Hauptteil" bezeichnet wird. Der Anfangsblock und der Hauptteil werden zusammen als die Gesiegelte COIN bezeichnet. Ein Benutzer führt die Gesiegelte COIN zusammen mit einer Berechtigung dem Zugriffsgerät zu, um einen Zugriff auf die COIN durchzuführen. Diese Berechtigung wird als "Siegelöffner" oder nur "Öffner" zu Vereinfachungszwecken bezeichnet. Die Öffner werden von dem Informationslieferanten auf Anforderung von dem Benutzer ausgegeben. Die Figuren 7A und 7B zeigen mögliche logische Strukturen der Gesiegelten COIN und des

Siegelöffners zur Verwirklichung der zweiten Ausführungsform der vorliegenden Erfindung. Nachfolgend werden Definitionen spezieller Ausdrücke und Kurzworte angegeben, die für den Rest der Beschreibung benötigt werden:

COIN	Originale Information, die in irgendeinem Digitalformat codiert ist und durch eine eindeutige Identifikation IID identifiziert ist.
TAL	Gesamtzahl von legalen Zugriffen auf die COIN, die der Informationslieferant dem Informationsverbraucher genehmigt.
LAL	Anzahl der verbleibenden legalen Zugriffe.
LAD	Das Gerät, an dem auf die COIN legal zugegriffen werden kann.
PID	eindeutige Identifikationsnummer des Informationslieferanten.
UID	Eindeutige Identifikationsnummer des Informationsverbrauchers.
CID	Eindeutige Identifikation eines Vertrages über die Informationsverbreitung. Logischerweise setzt ein Vertrag PID, IID, TAL, LAD und UID zueinander in Beziehung.
AW	Zugriffsfenster ist die Zeit, während der ein legaler Zugriff auf die COIN gewährt wird.

Eine Vereinbarung oder ein Vertrag zur Informationsverbreitung (CID) zwischen einem Informationslieferanten und einem Informationsverbraucher sieht zumindest vor, daß der Informationslieferant irgendeine COIN dem Informationsverbraucher für eine Anzahl von TAL legalen Zugriffen auf einem bestimmten LAD zur

Verfügung stellt. Damit steht CID zu PID, IID, TAL, LAD bzw. UID in Beziehung. In der einfachsten Form wird eine CID durch eine Verkettung von PID, IID, TAL, LAD und UID gebildet, wie dies logisch in Figur 7A gezeigt ist. Es ist für den Fachmann verständlich, daß, obwohl die Felder 121 bis 129 nach Fig. 7A in einer bestimmten Reihenfolge dargestellt sind, die Struktur von CID 120 in irgendeiner gerätemäßigen Ausführung nicht an diese Reihenfolge und Anordnung gebunden ist. In ähnlicher Weise ist die Allgemeinheit der vorhergehenden Komentare auf Fig. 7B anwendbar. CID 120 läuft ab, wenn die gesamten Zugriffe der Anzahl TAL 125 von Zugriffen durchgeführt wurden.

Gemäß erneuter Bezugnahme auf Figur 7A umfaßt die Gesiegelte COIN einen Anfangsblock 119 und einen Hauptteil 130. Wie dies weiter oben kurz erwähnt wurde, ist der Hauptteil 30 die ursprüngliche oder originale COIN, die unter Verwendung irgendeines Verschlüsselungsschemas codiert wurde, so daß der Erhalt der COIN ohne einen gültigen Entschlüsselungsschlüssel vom Rechenaufwand her nicht möglich ist. Der entschlüsselte Anfangsblock 119 umfaßt weiterhin drei Felder: CID 120, LAL 122 und Schlüssel 124. Die Schlüssel 124 bestehen aus der Anzahl von TAL Schlüsseln K_1, K_2, ..., K_{TAL}. Sie werden zum Entschlüsseln des Hauptteils und zur weiteren Verschlüsselung der COIN zur Bildung einer neuen Gesiegelten COIN verwendet.

Figur 7B zeigt die logische Struktur eines Siegelöffners. Dieser Siegelöffner weist ebenfalls einen Anfangsblock 140 und einen Hauptteil 145 auf. Der Anfangsblock 140 weist zwei Felder auf: CID 131 und AW 142. CID 131 des Öffners ist identisch zum CID 120 der Gesiegelten COIN. Das Feld AW 142 hält eine Anzahl von Zugriffsfenstern, während deren der Informationsverbraucher einen Zugriff auf die COIN ausführen kann. Der Hautpteil 145 enthält einen Entschlüsselungsschlüssel K_H für den Anfangsblock 119 der Gesiegelten COIN nach Fig. 7A. Der Schlüssel K_H wird für die Lebensdauer des Vertrages CID beibehalten. Für die zweite Ausführungsform der vorliegenden Erfindung wird ein Verschlüsselungsschema mit öffentlichem Schlüssel sowie ein übliches geheimes Schlüsselschema verwendet, um das Online-

Schema der Informationsverbreitung zu erläutern. Bezüglich des Schemas mit öffentlichem Schlüssel bezeichnet die vorliegende Erfindung die geheimen und öffentlichen Schlüssel des Informationslieferanten 10 mit PSK bzw. PPK, und die geheimen und öffentlichen Schlüssel des Zugriffsgerätes werden mit DSK bzw. DPK bezeichnet.

Figur 10 zeigt den logischen Ablauf des Gesamtverfahrens der kontrollierten Online-Verbretung von Information gemäß der vorliegenden Erfindung. Das Online-Schema der vorliegenden Erfindung beginnt mit dem Schließen eines Vertrages zwischen einem Informationslieferanten 10 und einem Informationsverbraucher 30 im Schritt 168 nach Figur 10. An diesem Punkt werden eine CID und ihre zugehörigen Felder PID 121, IID 123, TAL 125, LAD 127 und UID 129 in dem Vertrag vereinbart. Auf der Grundlage dieser Information erzeugt der Informationslieferant 10 eine gesiegelte COIN, wie dies in Figur 8 gezeigt ist, und überträgt sie über den Übertragungskanal 20 an den Informationsverbraucher im Schritt 170 nach Figur 10. Der Informationsverbraucher macht dann eine Anforderung über den gleichen Kanal an den Informationslieferanten 10 im Schritt 172 nach Figur 10. Nach der Überprüfung der Informationsanforderung durch den Verbraucher im Schritt 174 nach Figur 10 erzeugt der Informationslieferant 10 einen Öffner, wie dies in den Schritten 160 bis 166 nach Figur 9 umrissen ist, und überträgt den Öffner im Schritt 174 in Figur 10 an den Informationsverbraucher. Der Informationsverbraucher liefert die bereits früher empfangene gesiegelte COIN und den Öffner an das Steuergerät 48, um einen Zugriff auf die COIN im Schritt 176 durchzuführen.

Bei der Bestimmung, ob der Anforderung des Verbrauchers auf einen Zugriff im Schritt 178 stattgegeben werden soll, wendet das Steuergerät 48 die logische Folge von Schritten an, wie sie in den Figuren 11A und 11B umrissen sind, und deren Einzelheiten weiter unten erläutert werden. Wenn ein Zugriff gewährt wird, prüft das Steuergerät 48 im Schritt 182 nach Figur 10, ob der CID-Vertrag abgelaufen ist, d.h. ob die gesamte

Anzahl TAL von Zugriffen von dem Informationsverbraucher durchgeführt wurde. Wenn diese nicht der Fall ist, wird die COIN erneut gesiegelt, wie dies weiter unten beschrieben wird, und als Ergebnis wird dem Informationsverbraucher über den Informationsausgangskanal 29 zugänglich gemacht. Der Informationsverbraucher speichert die erneut gesiegelte COIN für einen späteren Zugriff im Schritt 184. Für nachfolgende Zugriffe beginnt der Informationsverbraucher mit dem Schritt 172, wobei er eine weitere Zugriffsanforderung an den Informationslieferanten 10 macht. Dies wird bis zum Ablauf des Vertrages im Schritt 180 fortgesetzt.

2. Erstellung der Gesiegelten COIN und des Siegelöffners

Figur 8 beschreibt, wie ein Informationslieferant eine Gesiegelte COIN erzeugt. Der Informationslieferant ist zur Erzeugung einer Gesiegelten COIN im Schritt 150 bereit, wenn er die CID und die Werte der zugehörigen Größen zur Verfügung hat, nämlich PID, IID, TAL, LAD und UID. Der Informationslieferant erzeugt als erstes eine Anzahl TAL von Schlüsseln K_1, K_2, ..., K_{TAL} im Schritt 152. Als nächstes bildet der Informationslieferant im Schritt 154 die Anfangsblock-Felder 119 der gesiegelten COIN durch Kombinieren des CID für das Feld 120, des Wertes von TAL für das Feld 122 und der Schlüssel für das Feld 124. Dann wird der Hauptteil 130 der Gesiegelten COIN durch Verschlüsseln der durch IID identifizierten COIN mit dem Schlüssel K_1 gebildet. Die Anfangsblock-Felder 119 werden ihrerseits im Schritt 156 verschlüsselt, um einen Anfangsblock mit einem neuen Schlüssel K_H zu bilden, den der Informationslieferant in Verbindung mit dem Vertrags-CID während der Laufzeit des Vertrages beibehält. Wie dies weiter oben erwähnt wurde, bildet der Schlüssel K_H einen Teil des Hauptteils des Öffners. Schließlich bildet der Informationslieferant die Gesiegelte COIN durch Verknüpfen des Anfangsblockes und des Hauptteils im Schritt 158.

Figur 9 zeigt im einzelnen die Schritte, mit denen der Informationslieferant einen Öffner erzeugt. Das Verfahren beginnt

damit, daß ein Informationsverbraucher eine Zugriffsanforderung mit einer gültigen CID und einer Anzahl von gültigen Zugriffsfenstern AW im Schritt 160 macht. Mit der CID findet der Informationslieferant den entsprechenden Schlüssel K_H, der im Schritt 156 dazu verwendet wird, die Anfangsblock-Felder 119 der Gesiegelten COIN zu verschlüsseln, und er verschlüsselt K_H unter Verwendung des geheimen Schlüssels PSK des Informationslieferanten im Schritt 162. Der Informationslieferant bildet dann den Öffner durch Verwenden der CID für das Feld 121, der AW-Werte für das Feld 142 und der vorstehend verschlüsselten K_H 144 im Schritt 164. Schließlich wird der Öffner durch Verschlüsseln des vorstehenden Ergebnisses mit dem öffentlichen Schlüssel DPK des Zugriffsgerätes im Schritt 166 erzeugt.

3. Zugriff auf Gesiegelte COIN

Wie dies weiter oben kurz erwähnt wurde, beschreiben die Figuren 11A und 11B die logischen Schritte des Steuergerätes bei der Bestimmung, ob der Zugriffsanforderung des Informationsverbrauchers stattgegeben werden soll. Der Schritt 200 prüft, ob der Eingang nicht-kontrollierte Information ist. Ein Beispiel nicht-kontrollierter Information sind Kataloginformationen, die der Benutzer durchsuchen kann. Wenn der Eingang eine nicht-kontrollierte Information ist, wird sie an die Ausgangseinheit 50 über den freien Kanal 47 abgegeben. Anderenfalls fragt das Steuergerät 48 den Informationsverbraucher im Schritt 204 nach einem Öffner. Das Steuergerät verwendet seinen eigenen geheimen Schlüssel DSK (d.h. den des Zugriffsgerätes), um den Öffner zu entschlüsseln, um die CID und die AW-Werte aus dem Feld 131 und dem Feld 142 im Schritt 206 abzuleiten. Aus der CID leitet das Steuergerät die LAD aus dem Feld 127 ab. Das Steuergerät prüft, ob die LAD mit seiner eigenen Identifikation (d.h. der des Zugriffsgerätes) übereinstimmt, und überprüft, ob die derzeitige Zeit entsprechend dem Takt 55 innerhalb einer der AW-Werte lieft, die sich in dem Feld 142 finden. Wenn irgendeine dieser Prüfungen fehlschlägt, wird der Zugriff auf die kontrollierte Information im Schritt 210 verweigert.

Wenn die Prüfungen im Schritt 208 erfolgreich sind, leitet das Steuergerät die PID aus dem Feld 121 und somit den öffentlichen Schlüssel PPK des Informationslieferanten im Schritt 212 ab. Mit diesem Schlüssel entschlüsselt das Steuergerät den Hauptteil 145 des Öffners, um K_H im Schritt 214 zu gewinnen. Unter Verwendung von K_H entschlüsselt das Steuergerät dann im Schritt 216 den Anfangsblock 119 der Gesiegelten COIN, die vorher von dem Informationsverbraucher dargeboten wurde. Dann leitet es den Wert von TAL aus dem Feld 125 des Anfangsblockes im Schritt 218 ab. Das Steuergerät prüft dann im Schritt 220, ob T (der Wert von TAL - LAL + 1) innerhalb des Bereiches von [1,TAL] liegt. Im Schritt 222 wird der Zugriff verweigert, wenn T nicht innerhalb des Bereiches liegt. Wenn T innerhalb des Bereiches leigt, prüft das Steuergerät dann, ob der T-te Zugriff im Schritt 224 in Figur 11B durchgeführt wurde. Es ist wichtig, festzustellen, daß der T-te Zugriff in dem Speicher 52 im Schritt 231 aufgezeichnet wird. Die zweiten und nachfolgenden Versuche für den T-ten Zugriff werden im Schritt 222 abgwiesen. Wenn der T-te Zugriff noch nicht durchgeführt wurde, entschlüsselt das Steuergerät dann den Hauptteil 130 der Gesiegelten COIN unter Verwendung des Schlüssels K_T, der sich in dem Feld 124 des Anfangsblockes findet. Das Steuergerät sendet das Ergebnis an die Ausgangseinheit 50 über den Freikanal 47 im Schritt 226. Wenn LAL größer als 1 ist, geht das Steuergerät 230 über. Hier verschlüsselt das Steuergerät erneut die COIN unter Verwendung des Schlüssels K_{T+1}, der sich im Feld 124 des Anfangsblockes 119 findet. Als nächstes verkleinert das Steuergerät den Wert im Feld 122 des Anfangsblockes 119 um 1 und verschlüsselt den neuen Anfangsblock unter Verwendung des Schlüssels K_H. Der Anfangsblock 119 wird somit zu dem modifizierten Anfangsblock 119'. Der modifizierte Anfangsblock 119 und COIN werden miteinander verknüpft, um eine neue Gesiegelte COIN zu bilden, die dem Informationsausgangskanal 29 zugeführt wird, damit die Information gespeichert wird. Schließlich wird im Schritt 231 der derzeitige Wert von AL in dem Speicher 52 für die Prüfung im Schritt 224 gespeichert, ob der T-te Zugriff durchgeführt wurde. Das Verfahren endet im Schritt 232.

Obwohl die vorliegende Erfindung hauptsächlich unter Bezugnahme auf die Figuren 1 und 11B mit besonderer Betonung eines Verfahrens zur Steuerung der Verbreitung von digitaler Information entweder im Offline- oder Online-Betrieb beschrieben wurde, ist es verständlich, daß die Figuren lediglich zu Erläuterungszwecken dienen und nicht als Beschränkung der Erfindung aufgefaßt werden sollten. Zusätzlich ist es klar, daß die Verfahren der vorliegenden Erfindung bei vielen Anwendungen brauchbar sind, bei denen eine Kontrolle der Verbreitung digitaler Information erforderlich ist.

95301630.0
EP 0672991

5 Patentansprüche

1. Verfahren zur Schaffung einer verbesserten Kontrolle über den Gebrauch kontrollierter Information in einem System zur 10 Steuerung der Verbreitung von Information durch einen Informationslieferanten im Offline-Betrieb, unter Einschluß von zumindest einem Speichermedium und einer Zugriffseinrichtung, die einem Informationsverbraucher zur Verfügung steht, wobei die Information sowohl kontrollierte Information oder COIN 15 als auch unkontrollierte Information einschließt, mit den folgenden Schritten:

a) Verschlüsseln der COIN und eines Anfangsblockes zur Erzeugung einer gesiegelten COIN auf dem Speichermedium, wobei der Anfangsblock zumindest eine Gesamtzahl von 20 rechtmäßigen Zugriffen, eine Anzahl von verbleibenden rechtmäßigen Zugriffen, eine Vielzahl von Verschlüsselungs-/Entschlüsselungs-Schlüsseln und eine Medium-Signatur zur Prüfung und Validierung der Authentizität des Speichermediums umfaßt,

25 b) Entschlüsselung des Anfangsblockes der gesiegelten COIN Prüfen der Werte in dem Anfangsblock mit einem Steuergerät, das in der Zugriffseinrichtung angeordnet ist, beim Zugriff auf das Speichermedium durch einen Informationsverbraucher, wobei das Steuergerät den Zugriff 30 auf die Information verweigert, wenn irgendeine der Prüfungen fehlschlägt,

c) Entschlüsseln der COIN unter Verwendung eines der Verschlüsselungs-/Entschlüsselungs-Schlüssel und Zuführung der COIN-Information zu einer Ausgabeeinheit, 35 die in der Zugriffseinrichtung angeordnet ist, wenn alle von dem Steuergerät in b) durchgeführten Prüfungen erfolgreich sind, wobei der Anfangsblock modifiziert wird, um zu einem modifizierten Anfangsblock derart

zu werden, daß die Anzahl der verbleibenden Zugriffe abwärts gezählt wird, und

d) Neuverschlüsseln der COIN und des modifizierten Anfangsblockes unter Verwendung eines anderen der Verschlüsselungs-/Entschlüsselungs-Schlüssel nach jeder Zugriffsanforderung von dem Informationsverbraucher, bis kein rechtmäßiger Zugriff verblieben ist;

wodurch der Informationslieferant eine Kontrolle des Zugriffs durch Festsetzen von Werten für den Anfangsblock entsprechend der Vereinbarung zwischen dem Informationslieferanten und dem Informationsverbraucher ausübt und der Informationsverbraucher in transparenter Weise einen Zugriff auf kontrollierte und unkontrollierte Information ausführt.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß der Anfangsblock weiterhin eine Vielzahl von Zugriffsfenstern umfaßt, wobei der Wert jedes dieser Zugriffsfenster von dem Steuergerät geprüft wird, um den Zugriff auf die Information während einer vorgegebenen Zeitperiode zuzulassen.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet, daß die Medium-Signatur den Zugriff auf die Information auf der Zugriffseinrichtung lediglich dann ermöglicht, wenn das Steuergerät eine Übereinstimmung der Medium-Signatur des Speichermediums mit der Medium-Signatur ergibt, die von der Zugriffseinrichtung gelesen wird.

4. Verfahren zur Schaffung einer verbesserten Kontrolle über den Gebrauch kontrollierter Information in einem System zur Steuerung der Verbreitung von Information durch einen Informationslieferanten in einer Online-Weise über zumindest einen Übertragungskanal und zumindest eine Zugriffseinrichtung, die einem Informationsverbraucher zur Verfügung steht, wobei die Information sowohl kontrollierte Information oder COIN als auch unkontrollierte Information einschließt, mit den folgenden Schritten:

a) Verschlüsselung der COIN und eines Anfangsblockes zur Erzeugung einer gesiegelten COIN, bevor die gesiegelte COIN an den Informationsverbraucher gesandt wird, wobei der Anfangsblock zumindest eine Gesamtzahl von rechtmäßigen Zugriffen, eine Anzahl von verbleibenden rechtmäßigen Zugriffen, eine Vielzahl von Verschlüsselungs-/Entschlüsselungs-Schlüsseln zur Verschlüsselung der Information umfaßt, wobei der Anfangsblock mit einem Verschlüsselungs-/Entschlüsselungs-Schlüssel K_H verschlüsselt ist, der für die Laufzeit eines vorgegebenen Verteilungsvertrages aufrechterhalten wird,

b) Verschlüsseln einer Versiegelungsfreigabe bei Empfang einer Zugriffsanforderung von einem Informationsverbraucher und Senden der Versiegelungsfreigabe an den Informationsverbraucher, wobei die Versiegelungsfreigabe zumindest eine Vielzahl von Zugriffsfenstern und den Schlüssel K_H umfaßt,

c) Entschlüsseln der Versiegelungsfreigabe mit einem in der Zugriffseinrichtung angeordneten Steuergerät, wobei das Steuergerät das Zugriffsfenster in der Versiegelungsfreigabe bei Zugriff durch den Informationsverbraucher prüft und das Steuergerät einen Zugriff auf die Information verweigert, wenn eine der Prüfungen fehlschlägt,

d) Enschlüsseln des Anfangsblockes der gesiegelten COIN und Prüfen der Werte in dem Anfangsblock mit einem in der Zugriffseinrichtung angeordneten Steuergerät bei Zugriff auf die Information durch einen Informationsverbraucher, wobei das Steuergerät den Zugriff auf die Information verweigert, wenn eine der Prüfungen fehlschlägt,

e) Entschlüsseln der COIN unter Verwendung eines der Verschlüsselungs-/Entschlüsselungs-Schlüssel und Lieferung der darin enthaltenen Information an eine Ausgabeeinheit, die in der Zugriffseinrichtung angeordnet ist, wenn alle die von dem Steuergerät in d) gemachten Prüfungen erfolgreich sind, wobei der Anfangsblock modifiziert wird, um zu einem modifizierten Anfangsblock derart zu werden, daß die Anzahl der verbleibenden Zugriffe abwärts gezählt wird,

f) erneutes Verschlüsseln der COIN und des modifizierten Anfangsblockes unter Verwendung eines anderen der Verschlüsselungs-/Entschlüsselungs-Schlüssel nach jeder Zugriffsanforderung von dem Informationsverbraucher, bis kein rechtmäßiger Zugriff verblieben ist,

wodurch der Informationslieferant eine Kontrolle des Zugriffs dadurch ausübt, daß Werte für den Anfangsblock entsprechend der Vereinbarung zwischen dem Informationslieferanten und dem Informationsverbraucher gesetzt werden und der Informationsverbraucher in transparenter Weise einen Zugriff auf kontrollierte und unkontrollierte Information ausführt.

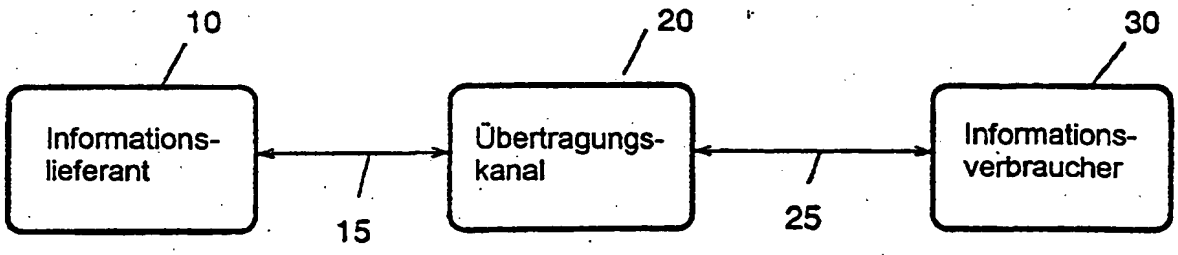
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Information digitale Information umfaßt.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das Steuergerät eine vorgegebene Anzahl von Zugriffen auf die Information nach der Prüfung des Wertes der Gesamtzahl der verbleibenden rechtmäßigen Zugriffe ermöglicht.

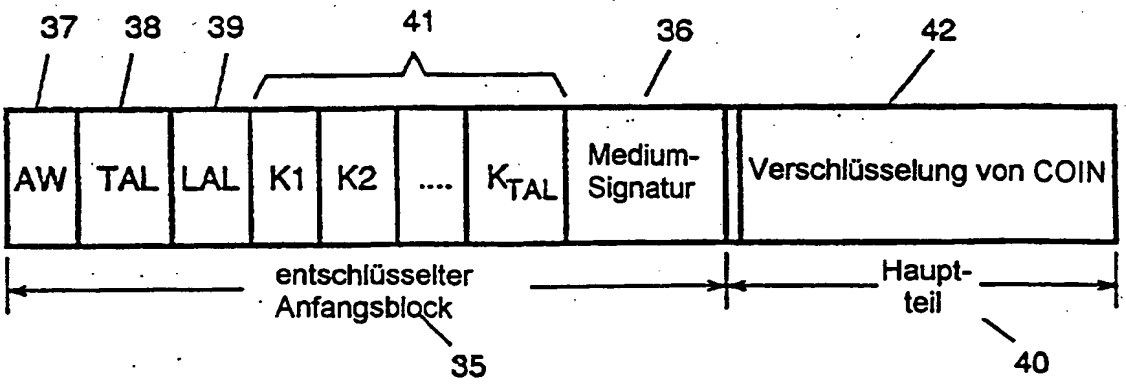
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß der Anfangsblock weiterhin Identifikationsinformation für eine rechtmäßige Zugriffseinrichtung umfaßt, wobei der Wert der rechtmäßigen Zugriffsinformation von dem Steuergerät geprüft wird, um einen Zugriff lediglich auf die rechtmäßige Zugriffseinrichtung zu ermöglichen.

8. Verfahren nach einem der Ansprüche 4 oder 5 bis 7 unter Rückbeziehung auf Anspruch 4, dadurch gekennzeichnet, daß die Zugriffsfenster der Versiegelungsfreigabe durch das Steuergerät geprüft werden, um den Zugriff auf die Information nur während einer vorgegebenen Zeitperiode zuzulassen.

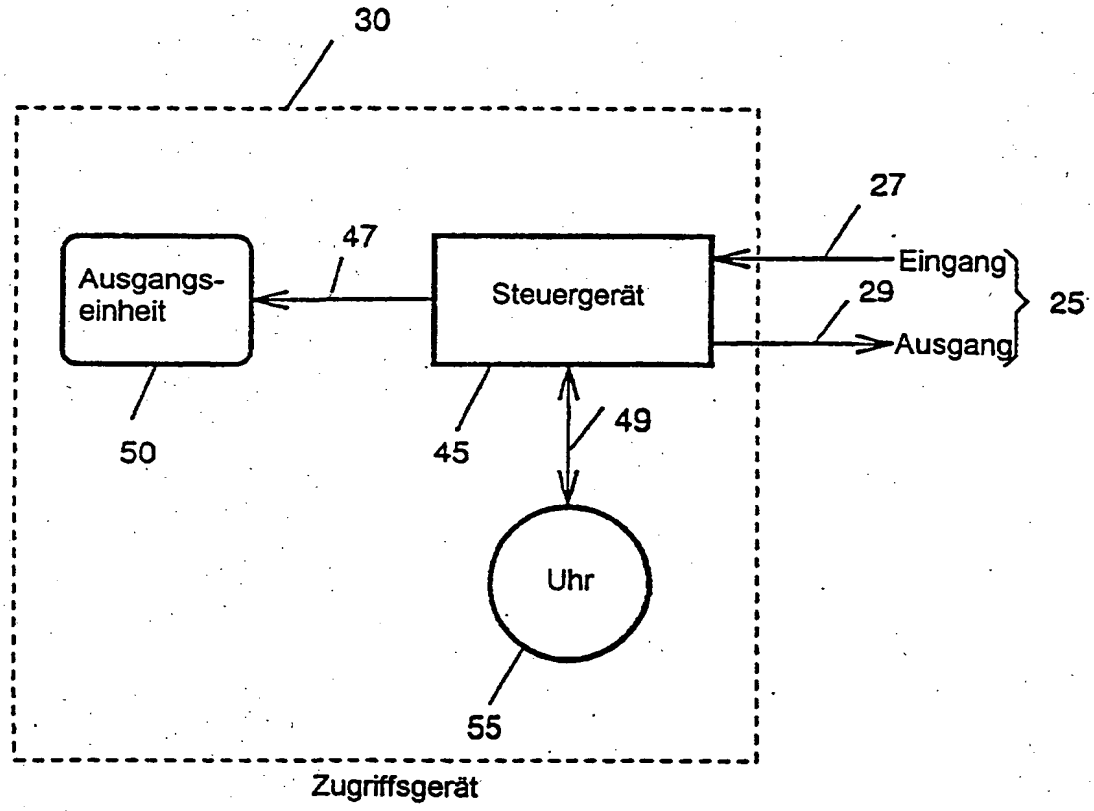
9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß das Steuergerät mit der Ausgabeeinheit über manipulierungssichere Verbindungen gekoppelt ist.



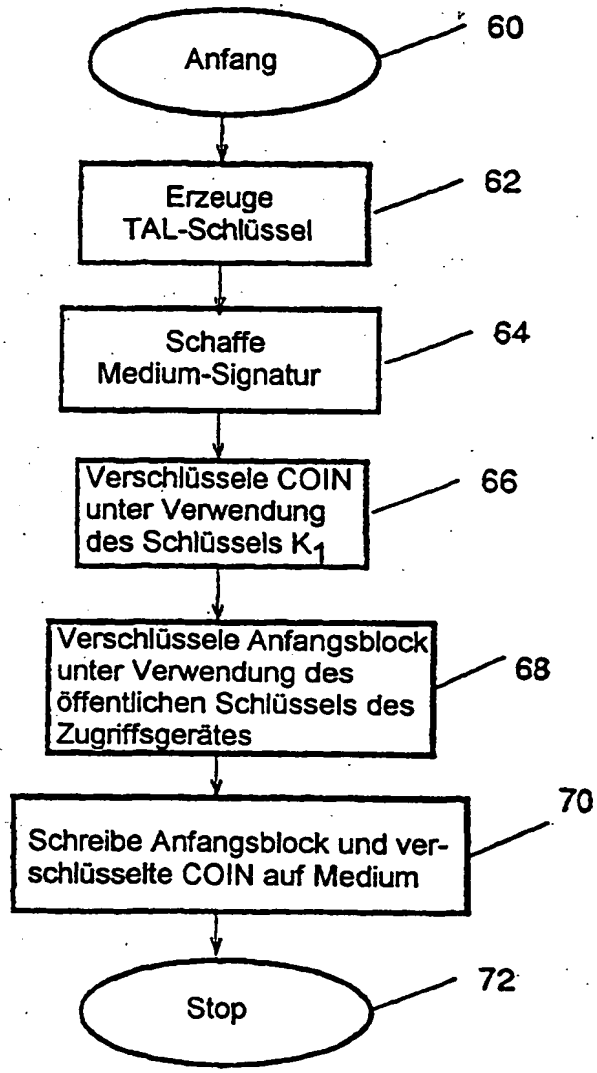
Figur 1



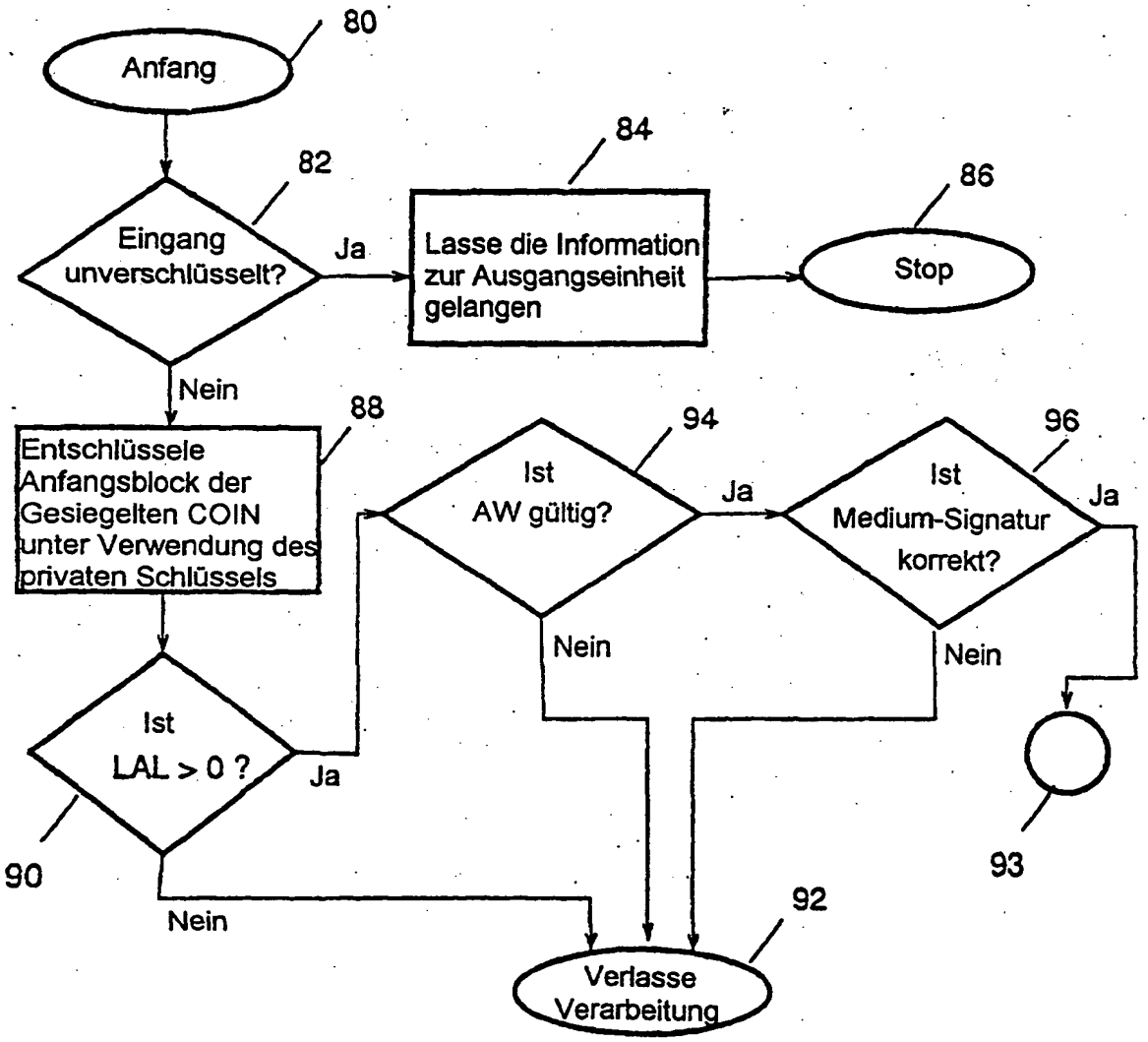
Figur 2


30
27
47
Ausgangs-
einheit
Steuergerät
Eingang
29
25
Ausgang
50
45
49
Uhr
55
Zugriffsgerät

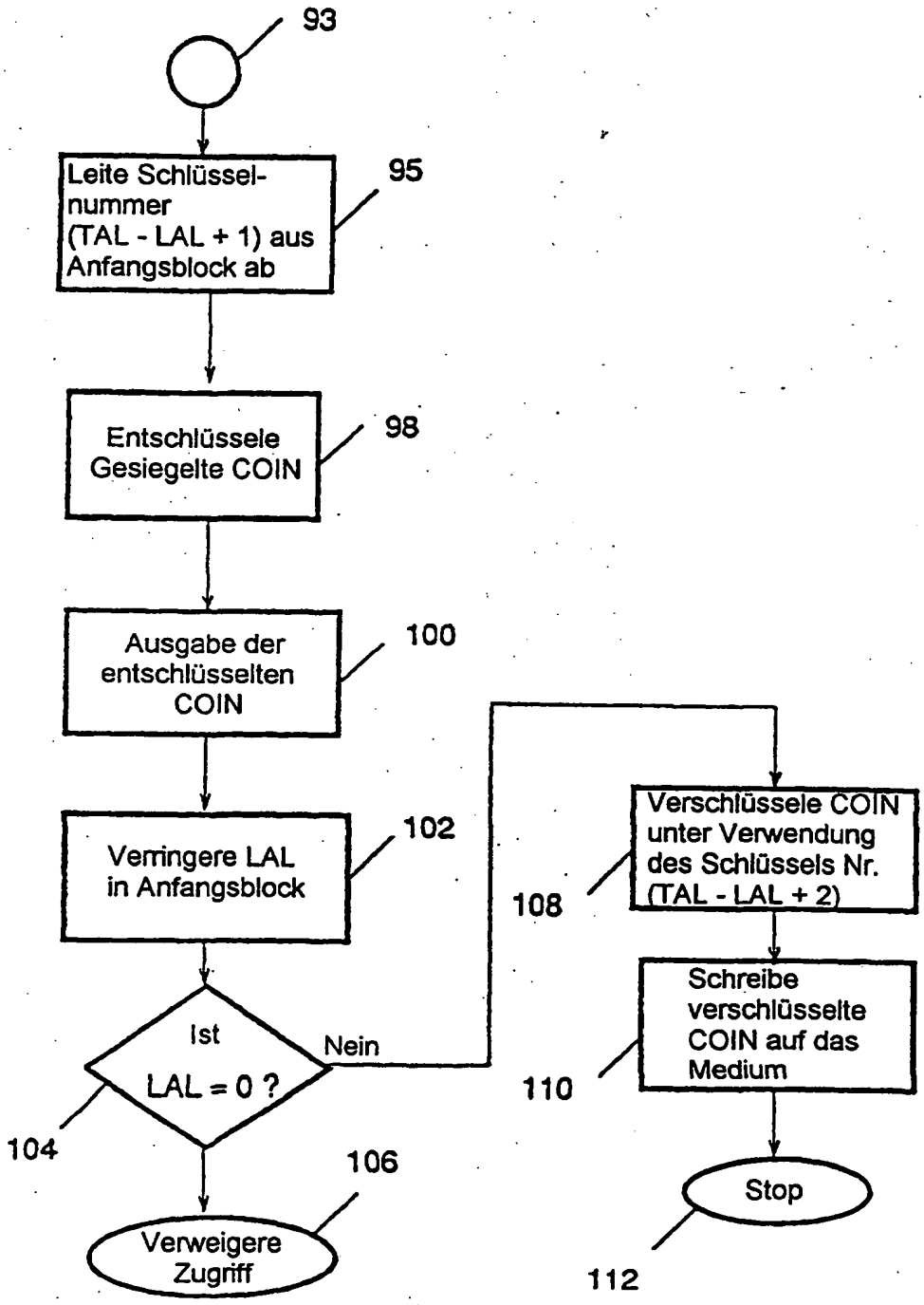
Figur 3


Anfang
60
Erzeuge TAL-Schlüssel
62
Schaffe Medium-Signatur
64
Verschlüssele COIN unter Verwendung des Schlüssels K_1
66
Verschlüssele Anfangsblock unter Verwendung des öffentlichen Schlüssels des Zugriffsgerätes
68
Schreibe Anfangsblock und verschlüsselte COIN auf Medium
70
Stop
72

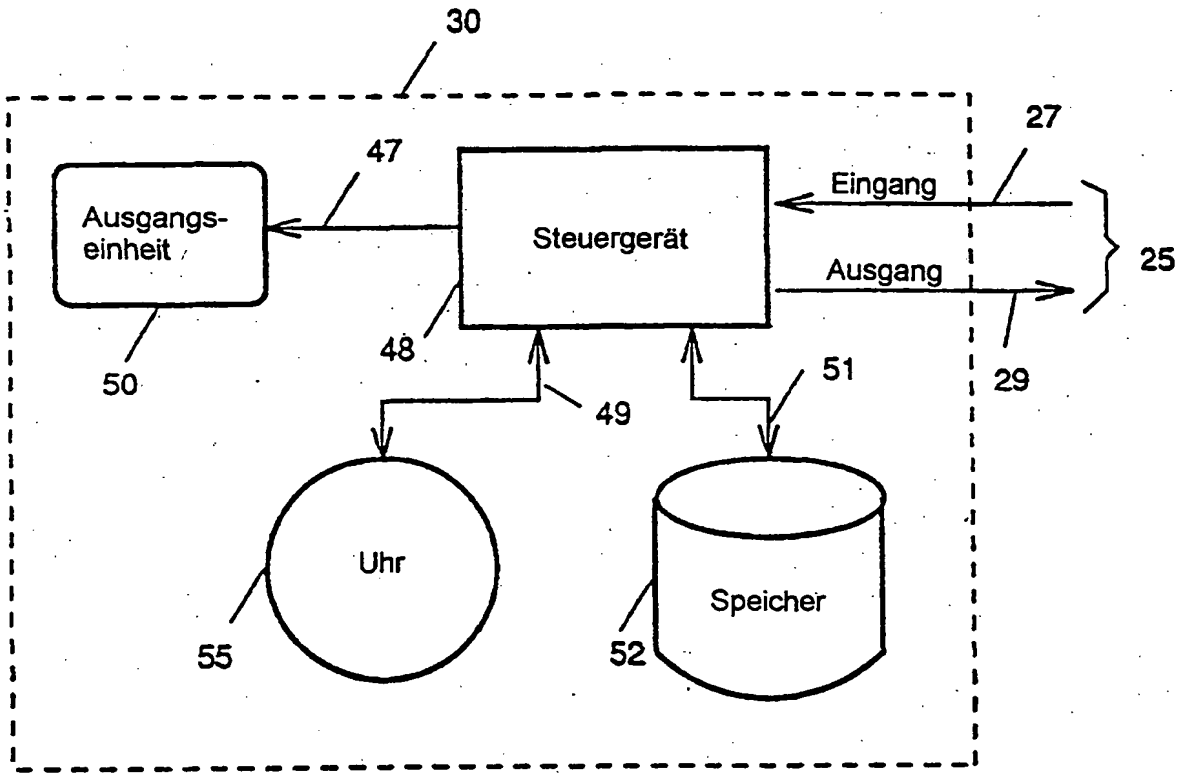
Figur 4


80
Anfang
82
Eingang unverschlüsselt?
Ja
84
Lasse die Information zur Ausgangseinheit gelangen
86
Stop
Nein
88
Entschlüssele Anfangsblock der Gesiegelten COIN unter Verwendung des privaten Schlüssels
94
Ist AW gültig?
Ja
96
Ist Medium-Signatur korrekt?
Ja
Nein
Nein
Ist LAL > 0 ?
Ja
90
Nein
92
Verlasse Verarbeitung
93

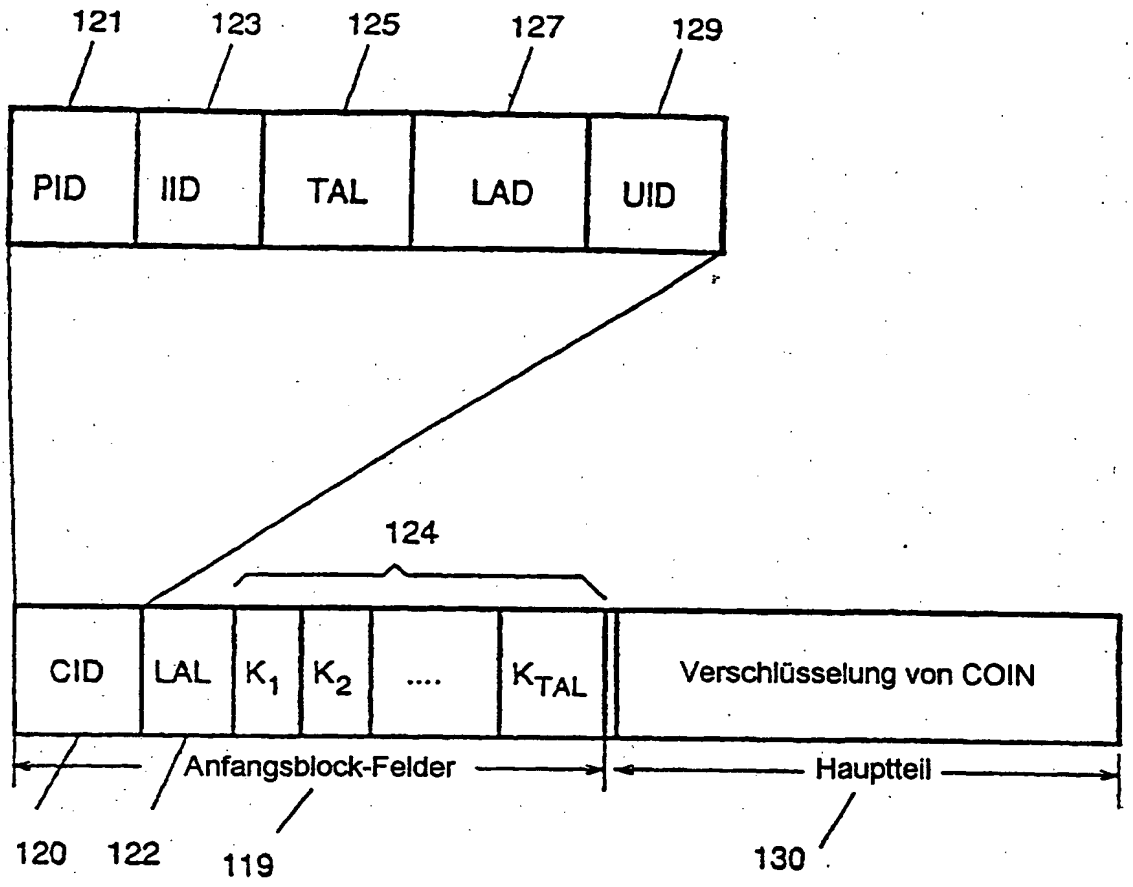
Figur 5A


93
Leite Schlüssel-nummer (TAL - LAL + 1) aus Anfangsblock ab
95
Entschlüssele Gesiegelte COIN
98
Ausgabe der entschlüsselten COIN
100
Verringere LAL in Anfangsblock
102
Ist LAL = 0 ?
Nein
104
Verweigere Zugriff
106
Verschlüssele COIN unter Verwendung des Schlüssels Nr. (TAL - LAL + 2)
108
Schreibe verschlüsselte COIN auf das Medium
110
Stop
112

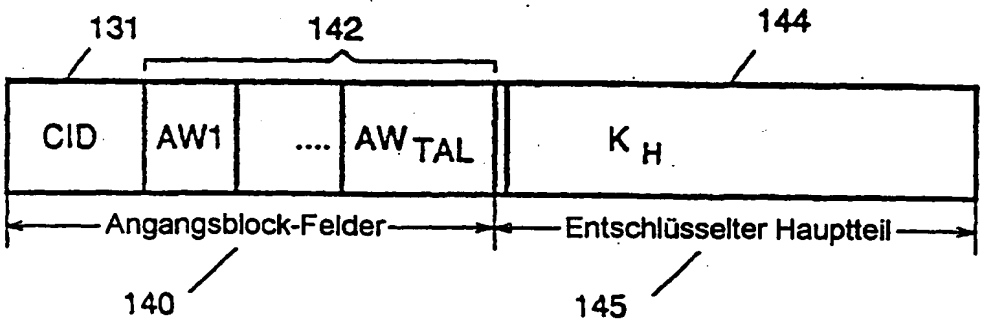
Figur 5B


30
27
47
Eingang
Ausgangs-
einheit
Steuergerät
25
Ausgang
48
50
29
51
49
Uhr
Speicher
55
52
Zugriffsgerät

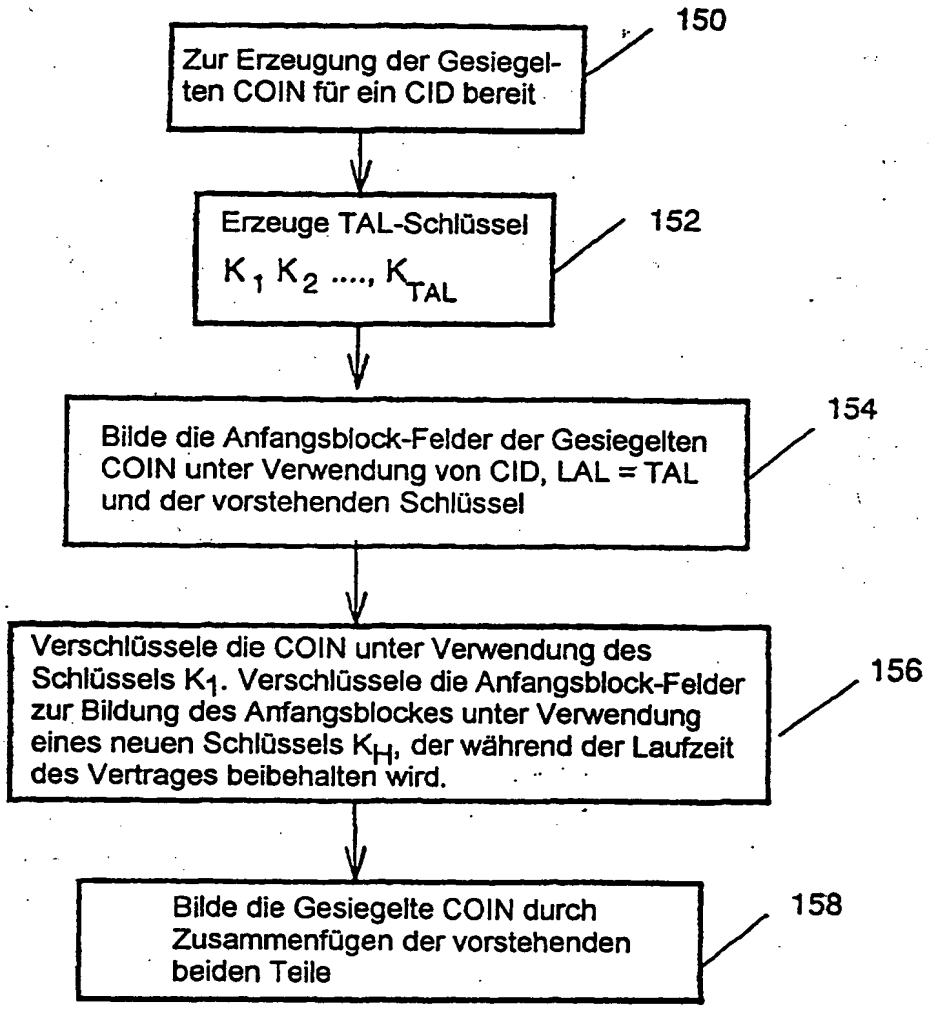
Figur 6



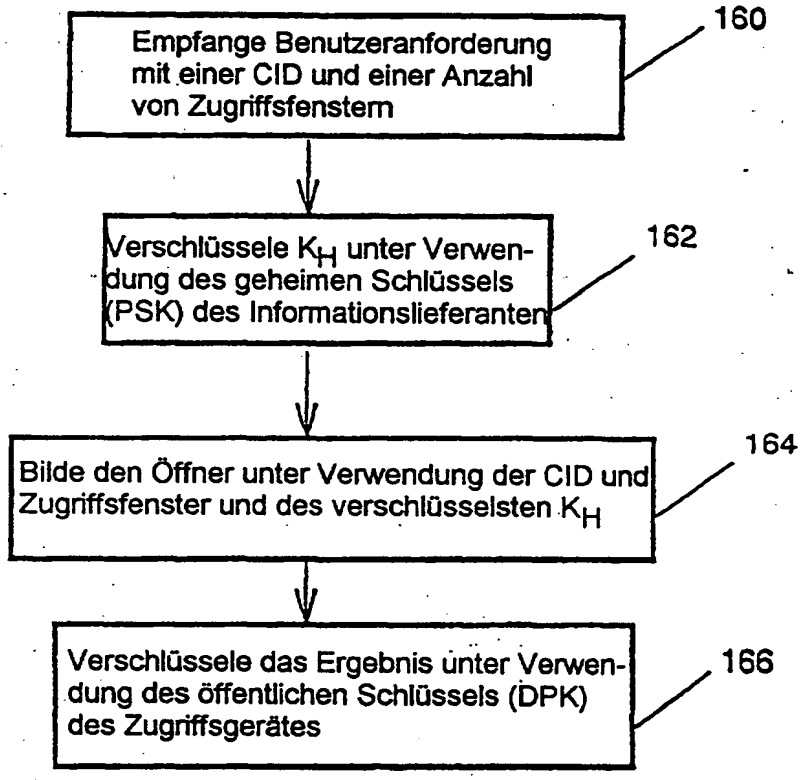
Figur 7A



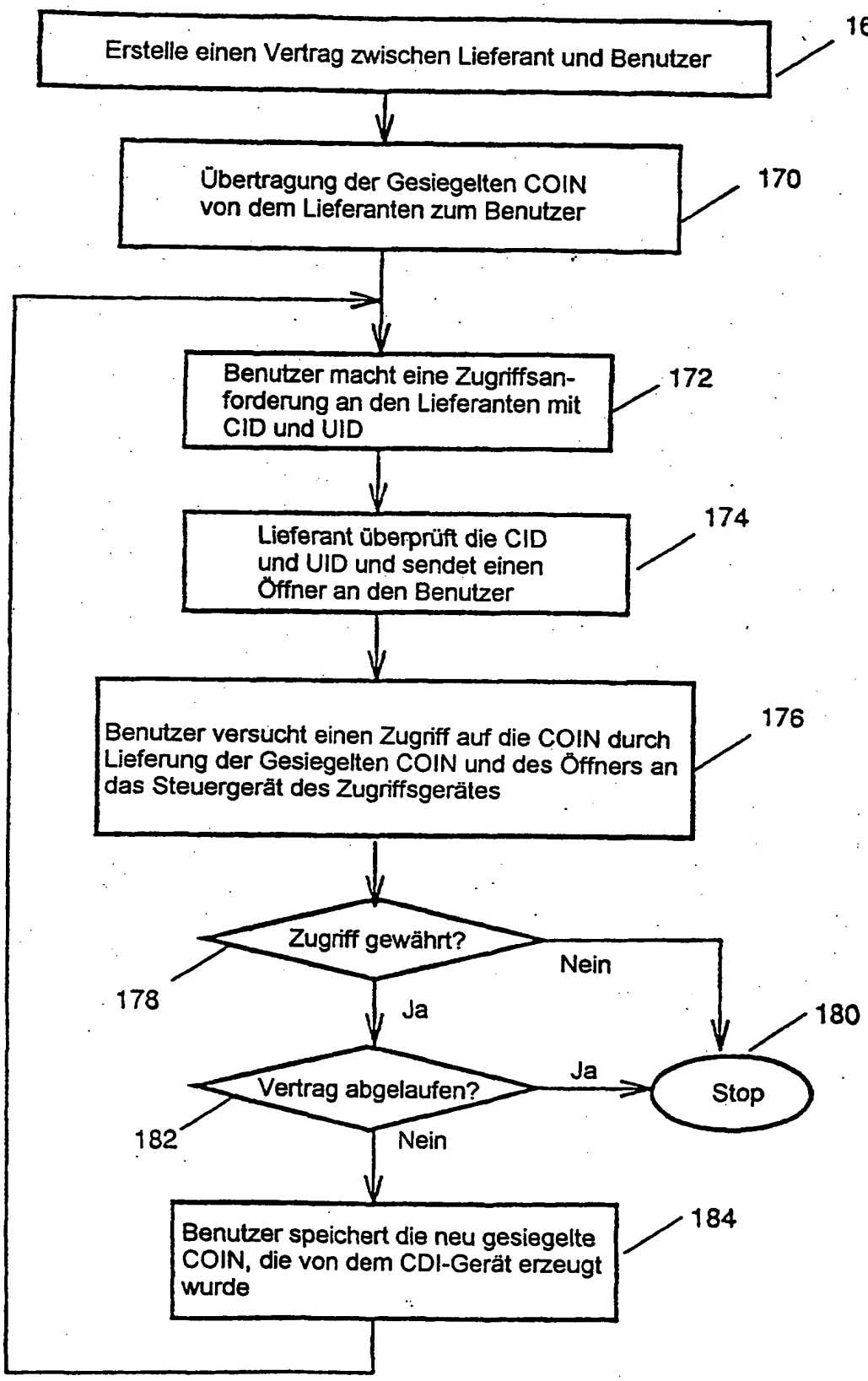
Figur 7B


150
Zur Erzeugung der Gesiegelten COIN für ein CID bereit
152
Erzeuge TAL-Schlüssel
$K_1 K_2 ...., K_{TAL}$
154
Bilde die Anfangsblock-Felder der Gesiegelten COIN unter Verwendung von CID, LAL = TAL und der vorstehenden Schlüssel
156
Verschlüssele die COIN unter Verwendung des Schlüssels K_1. Verschlüssele die Anfangsblock-Felder zur Bildung des Anfangsblockes unter Verwendung eines neuen Schlüssels K_H, der während der Laufzeit des Vertrages beibehalten wird.
158
Bilde die Gesiegelte COIN durch Zusammenfügen der vorstehenden beiden Teile

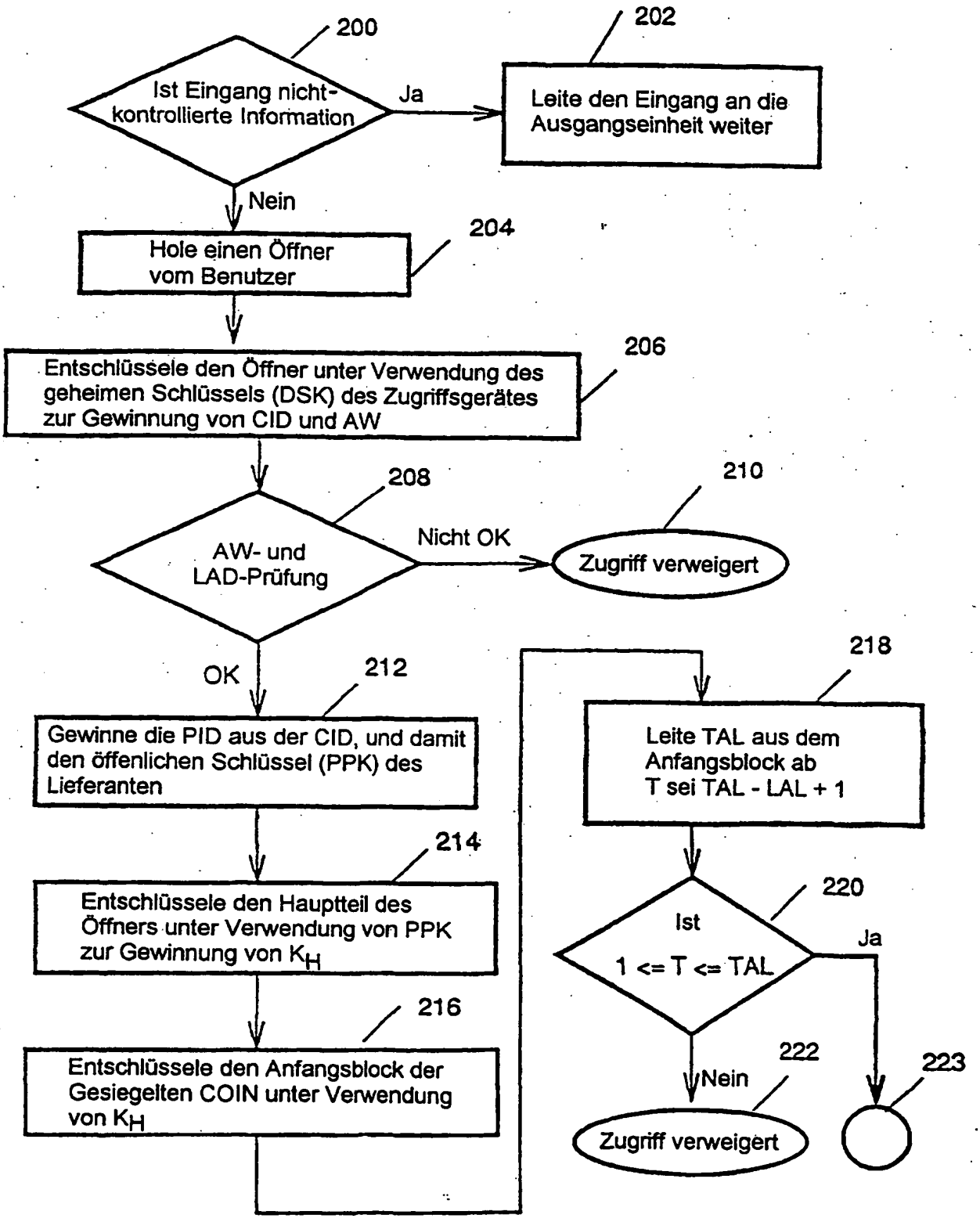
Figur 8


Empfange Benutzeranforderung mit einer CID und einer Anzahl von Zugriffsfenstern
160
Verschlüssele K_H unter Verwendung des geheimen Schlüssels (PSK) des Informationslieferanten
162
Bilde den Öffner unter Verwendung der CID und Zugriffsfenster und des verschlüsselsten K_H
164
Verschlüssele das Ergebnis unter Verwendung des öffentlichen Schlüssels (DPK) des Zugriffsgerätes
166

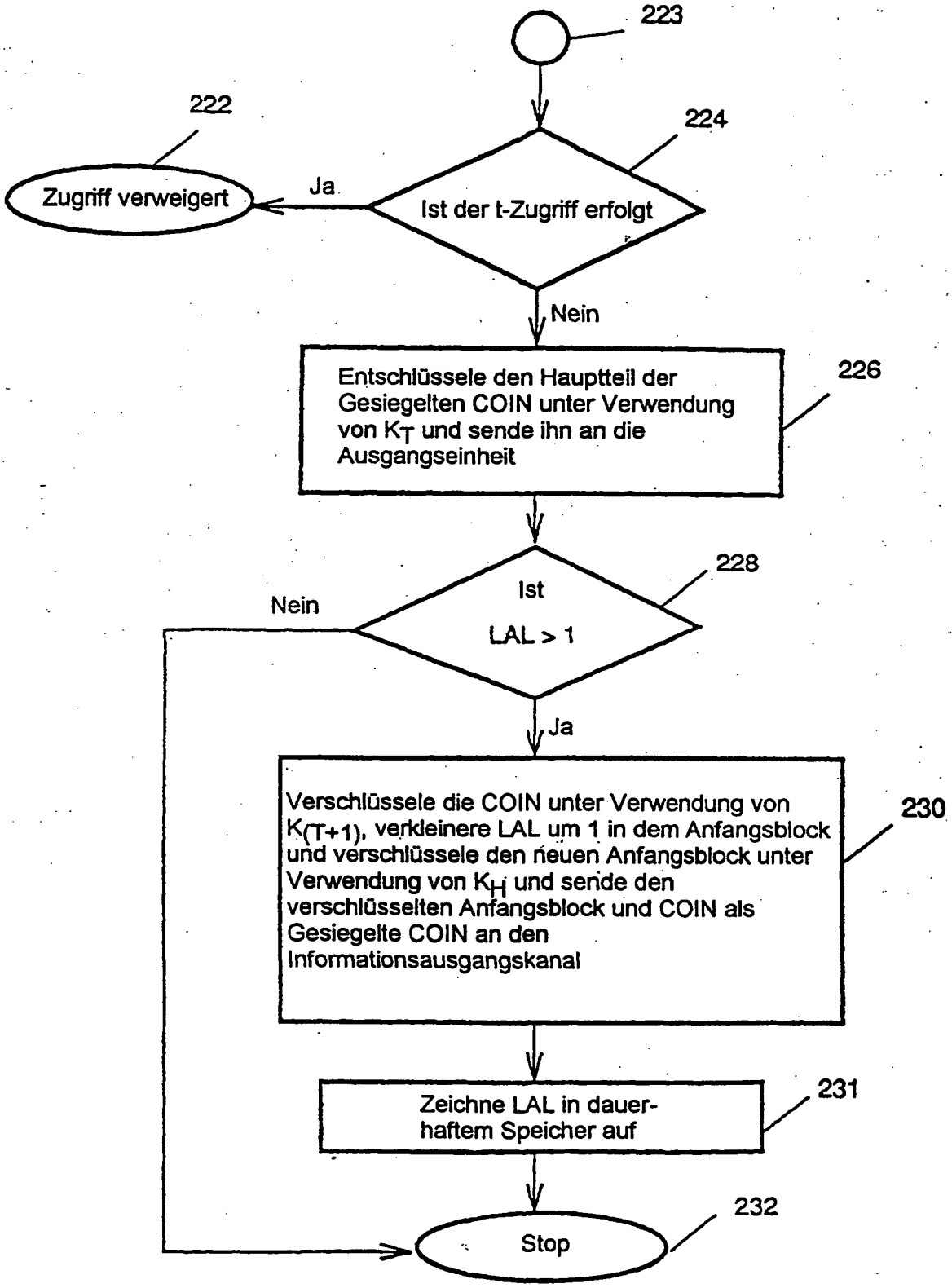
Figur 9


Erstelle einen Vertrag zwischen Lieferant und Benutzer
168
Übertragung der Gesiegelten COIN von dem Lieferanten zum Benutzer
170
Benutzer macht eine Zugriffsanforderung an den Lieferanten mit CID und UID
172
Lieferant überprüft die CID und UID und sendet einen Öffner an den Benutzer
174
Benutzer versucht einen Zugriff auf die COIN durch Lieferung der Gesiegelten COIN und des Öffners an das Steuergerät des Zugriffsgerätes
176
Zugriff gewährt?
178
Nein
Ja
180
Vertrag abgelaufen?
Ja
Stop
182
Nein
Benutzer speichert die neu gesiegelte COIN, die von dem CDI-Gerät erzeugt wurde
184

Figur 10


200
Ist Eingang nicht-kontrollierte Information
Ja
202
Leite den Eingang an die Ausgangseinheit weiter
Nein
204
Hole einen Öffner vom Benutzer
206
Entschlüssele den Öffner unter Verwendung des geheimen Schlüssels (DSK) des Zugriffsgerätes zur Gewinnung von CID und AW
208
AW- und LAD-Prüfung
Nicht OK
210
Zugriff verweigert
OK
212
Gewinne die PID aus der CID, und damit den öffenlichen Schlüssel (PPK) des Lieferanten
214
Entschlüssele den Hauptteil des Öffners unter Verwendung von PPK zur Gewinnung von K_H
216
Entschlüssele den Anfangsblock der Gesiegelten COIN unter Verwendung von K_H
218
Leite TAL aus dem Anfangsblock ab
T sei TAL - LAL + 1
220
Ist
1 <= T <= TAL
Ja
Nein
222
Zugriff verweigert
223

Figur 11A


223
222
224
Zugriff verweigert
Ja
Ist der t-Zugriff erfolgt
Nein
Entschlüssele den Hauptteil der Gesiegelten COIN unter Verwendung von K_T und sende ihn an die Ausgangseinheit
226
228
Nein
Ist
LAL > 1
Ja
Verschlüssele die COIN unter Verwendung von $K_{(T+1)}$, verkleinere LAL um 1 in dem Anfangsblock und verschlüssele den neuen Anfangsblock unter Verwendung von K_H und sende den verschlüsselten Anfangsblock und COIN als Gesiegelte COIN an den Informationsausgangskanal
230
Zeichne LAL in dauer-haftem Speicher auf
231
Stop
232

Figur 11B